A BŰNÜGYI TUDOMÁNYOK ÉS AZ INFORMATIKA

A BŰNÜGYI TUDOMÁNYOK ÉS AZ INFORMATIKA

Szerkesztette:
MEZEI KITTI

BUDAPEST–PÉCS, 2019.

Az Emberi Erőforrások Minisztériuma ÚNKP-18-3-IV kódszámú
Új Nemzeti Kiválóság Programjának támogatásával készült.

Kiadó: Pécsi Tudományegyetem Állam- és Jogtudományi Kar
– MTA Társadalomtudományi Kutatóközpont
Felelős kiadó: Fábián Adrián dékán – Boda Zsolt főigazgató
Szakmai lektor: Tóth Mihály DSc. egyetemi tanár, tudományos tanácsadó
Szerkesztő: Mezei Kitti

ISBN 978-963-429-364-4 (print)
ISBN 978-963-429-299-9 (elektronikus)

Borítóterv: Szefcsik Zoltán (Sz.Graphic)
Nyomdai munkálatok: Séd Kft., Szekszárd

TARTALOM

Előszó

A kötet célja interdiszciplináris keretek között áttekinteni a technológiai fejlődés következtében megjelenő új kihívásokat és az ezekre adható válaszokat a bűnügyi tudományokban. A szerzők ezeknek egy vagy több részterületével foglalkoznak, így a büntető anyagi joghoz vagy eljárásjoghoz, a kriminalisztikához, a kriminológiához és a rendészethez kapcsolódó kérdésekkel.

A büntető anyagi jogon belül a modern technológiák és az új elkövetési módok az egyes büntetendő cselekmények körével összefüggésben szabályozási és minősítési kérdéseket vetnek fel. Ambrus István az autonóm járművekkel kapcsolatos büntetőjogi felelősség kérdéseit érinti, Csák Zsolt pedig a drónok felhasználásával elkövethető bűncselekményeket értékeli, valamint kitér ezek eljárásjogi összefüggéseire is.

A hazai szakirodalom keveset foglalkozik a kiberbűnözéssel annak ellenére, hogy napjaink egyik legnagyobb kihívását jelenti ez a terület. A kötet írásainak egy részének fókuszában éppen ezért az interneten elkövethető bűncselekmények állnak. Gyaraki Réka és Mezei Kitti a szervezett bűnözéssel, Dornfeld László a kiberbűnözés és kiberterrorizmus kapcsolatával, míg Nagy Zoltán a csalás-jellegű cselekmények minősítésével foglalkozik az e-kereskedelem körében.

Az internet egy határon átívelő bűnözésnek ad teret, ezért ezzel kapcsolatban joghatósági és illetékességi kérdések várnak megválaszolásra, többek között erre tesz kísérletet Szathmáry Zoltán a hazai joggyakorlat tükrében. A digitalizáció szerepe felértékelődött az új büntető eljárásjogi törvényünk hatályba lépésével, így ennek részleteit Herke Csongor ismerteti. A nyomozást nehezítik a titkosítást és anonimitást biztosító technológiák, amelyek egyre inkább lehetővé teszik, hogy az elkövetők hatékonyan elrejtsék a személyazonosságukat. A digitális felderítés rejtelmeivel Fenyvesi Csaba foglalkozik a kriminalisztikai fejezetben.

Új területként jelent meg a blockchain technológia és az erre épülő kriptovaluták, amelyeket gyakran bűnelkövetési céllal használnak fel. Mindez a nyomozó hatóságokat is számos kérdés elé állítja, ezért Simon Béla a kriptovalutákkal kapcsolatos rendészeti válaszokat vizsgálja.

Ezúton is köszönet illeti a szerzőket, hogy tanulmányaikkal hozzájárultak a kötethez és bízunk abban, hogy ezek mind a téma iránt érdeklődőknek, mind a jogalkalmazóknak, mind pedig a joghallgatóknak hasznos adalékként fognak szolgálni a munkájuk és kutatásuk során. További célunk, hogy a kötet témáihoz kapcsolódó hasonló írásokat jelentessünk meg, így reményeink szerint jelen antológia egy könyvsorozat legelső állomása.

Pécs, 2019. május 21.

A Szerkesztő

AMBRUS ISTVÁN

AZ AUTONÓM JÁRMŰVEK ÉS A BÜNTETŐJOGI FELELŐSSÉGRE VONÁS AKADÁLYAI[1]

1. Bevezetés

A 21. századi technológiai modernizáció a büntetőjog tudománya számára számos, az eddigiekben jóformán ismeretlen kihívást teremtett. Az egyik legfontosabb ilyen a – leegyszerűsítve mesterséges intelligenciának tekinthető rendszerek[2] által működtetett/működtetendő – autonóm (önvezető) járművek problémája.[3] A büntető

[1] A tanulmány a GINOP-2.3.4-15-2016-00003 projekt keretében készült a Széchenyi István Egyetemen.

[2] Brożek, Bartosz – Jakubiec, Marek: On the legal responsibility of autonomous machines. Artifical Intelligence and Law 2017/3. 293-304. o.; Hage, Jeep: Theoretical foundations for the responsibility of autonomous agents. Artifical Intelligence and Law 2017/3. 255-271. o.

[3] Autonóm vagy önvezető járművek kapcsán az ún. SLAM technológiára (simultaneous localization and mapping) szokás hivatkozni, amelynek lényege, hogy egy térképet készít és frissít a jármű vonatkozásában, amelyen elhelyezi magát. Ugyanakkor ez egyelőre nem teszi lehetővé a teljes automatizációt, így szükséges az egyes fejlettségi szintek szerinti konkrét csoportosítása, amely a SAE szerint az alábbiak szerint alakul:

Az emberi vezető végez minden műveletet. Egy automata valamely módon segíti a vezetőt, pl. a kormányzásban vagy a gyorsításban, illetve a lassításban. Ilyenek pl. a már napjainkban is működő, maguktól beparkoló járművek, ahol a vezetőnek csupán fékeznie kell.

Az automata a vezetés során egyes műveleteket magától végez, amelyeket a vezető csak felügyel, míg a többit magától végzi. Eltérés az előzőtől például, hogy egy gyorsítást és egyben kormányzást végző autó ide tartozik, míg csak egy csak a sebességet automatizáló az 1) csoportba. Ide tartozik pl. az ACC (adaptive cruise control) technológia. A leglényegesebb határ a 2) és a 3) között húzódik; ezen a szinten az autó nemcsak a feladatot végzi el, hanem az ellenőrzést is, ugyanakkor az emberi sofőrnek készen kell állnia az irányítás átvételére, amikor a rendszer megkívánja. Jelenleg ide sorolható a Tesla szoftverének 8.1-es frissítése, amely egyes modellek számára lehetővé teszi az ún. „Autosteer" funkciót, amely – 80 mérföld/órás sebességig – az irányjelző kar lenyomására magától figyeli a sávváltás lehetőségét, ellenőrzi a holtteret, majd vált sávot; ugyanakkor a vezetőnek végig fognia kell a kormányt a folyamat során.

Az automata elvégzi és felügyeli is a vezetési feladatokat, az emberi vezető közreműködése nélkül képes irányítani magát, de csak meghatározott szituációkban. Az automata jármű vezetési képessége megegyezik egy átlagos, az autóvezetést elsajátított emberével.

Lásd U.S. Department of Transportation's New Policy on Automated Vehicles Adopts SAE International's Levels of Automation for Defining Driving Automation in On-Road Motor Vehicles. https://www.sae.org/news/3544/ [2018.12.01.]

anyagi jogban ugyanis a felelősségre vonás fundamentumát hagyományosan a természetes személy (ember) által megvalósított, büntetőtörvénybe ütköző és büntetendőséget/büntethetőséget kizáró okokkal nem érintett cselekmény képezte/képezi. Az említett nóvum kapcsán azonban minimálisan megkérdőjeleződik ezen alapok megléte. Eme tanulmányban erre figyelemmel, ezen, hamarosan várhatóan robbanásszerűen elterjedő közlekedési eszközök, illetve a büntető anyagi jog egy részterülete, a tágabb értelemben vett bűncselekmény-fogalomhoz kapcsolódó egyik főfogalom, a büntetőjogi felelősségre vonás akadályai problémakörét járom körbe.[4] A jogellenesség (társadalomra veszélyesség) vonatkozásában elsősorban negatív oldalról érdemes megközelíteni a kérdést, tehát a jogellenességet kizáró okok vizsgálatát kell elvégezni. Kiemelhető mindenekelőtt a jogos védelem, a végszükség, illetve az indokolt (megengedett) kockázatvállalás. A bűnösség kapcsán negatív oldalról, tehát a bűnösséget kizáró okok oldaláról az ittas vagy bódult állapotban elkövetett bűncselekményért való felelősség, valamint a tévedés kérdésköre igényel részletes kidolgozást.

2. Általános megállapítások

A büntethetőségi akadályokat a hatályos Btk. alapvetően három kategóriába sorolja. A büntethetőséget kizáró (illetve korlátozó) okok (Btk. IV. fejezet) mellett büntethetőséget megszüntető okokat (Btk. V. fejezet), valamint a büntetőjogi felelősségre vonás egyéb akadályait (Btk. VI. fejezet) különbözteti meg. E három okfajta között a különbség abban áll, hogy a büntethetőséget kizáró körülmények, illetve a büntetőjogi felelősségre vonás egyéb akadályai már a bűncselekmény elkövetésekor léteznek, tehát ilyen körülmények fennállása során elkövetett cselekmény elkövetése pillanatában sem büntethető. A büntethetőséget megszüntető okok a bűncselekmény megvalósulása után jelentkeznek, így az eredetileg büntethető cselekményért egy később bekövetkező körülmény folytán, utóbb mégsem lehet felelősségre vonni az elkövetőt. Hasonlóan lényeges összefüggés, hogy büntethetőséget kizáró ok fennforgása esetén a bűncselekmény anyagi jogi értelemben sem jön létre (ún. elsődleges büntethetőségi

[4] A kapcsolódó jogirodalomban lásd például Gless, Sabine – Silverman, Emily – Weigend, Thomas: If Robots Cause Harm, Who is to Blame? Self-driving Cars and Criminal Liability. New Criminal Law Review 2016/3. 412-436. o.; Gurney, Jeffrey K.: Sue my Car not Me: Products Liability and Accidents Involving Autonomous Vehicles. Journal of Law, Technology & Policy 2013/3. 247-277. o.; Lohmann, Melinda Florina: Liability Issues Concerning Self-Driving Vehicles. The European Journal of Risk Regulation 2016/2. 335-340. o.

akadályok). Ezzel szemben büntethetőséget megszüntető ok, vagy egyéb büntetőjogi felelősségre vonással kapcsolatos akadály kapcsán a bűncselekmény ugyan megvalósul, az elkövető felelőssége azonban nem állapítható meg (ezek összefoglalóan az ún. másodlagos büntethetőségi akadályok). Már itt szükséges utalni továbbá arra, hogy a Btk. IV. fejezet címében ugyan csupán a büntethetőséget kizáró (korlátozó) okokra utal, a részletszabályok valójában további distinkciót tesznek a cselekmény büntetendőségét és az elkövető büntethetőségét kizáró okok között. Szintén említendő, hogy az ún. jogellenességet kizáró okok körében nem csupán Btk.-ban rögzített, hanem szokásjogi úton érvényesülő akadálytípusokkal is találkozhatunk.

A büntethetőségi akadályokat a Gellér Balázs és Ambrus István társszerzőségében megjelent, új általános részi tankönyvben[5] az alábbiak szerint csoportosítjuk:

Büntethetőséget kizáró (korlátozó) okok:

Jogellenességet kizáró okok:

- A bíró (jogalkalmazó) alkotta jogellenességet kizáró okok
  - a sértett beleegyezése
  - az indokolt kockázat
  - a fegyelmezési jog
  - a hivatás gyakorlása
- A jogos védelem [Btk. 21. §, 22. § (1)-(2) bek.]
- A végszükség [Btk. 23. § (1) bek.]
- A jogszabály engedélye (Btk. 24. §)
- A Btk. Különös Részében meghatározott további okok

Bűnösséget kizáró okok:

- A gyermekkor
- A kóros elmeállapot
- A kényszer és a fenyegetés
- A tévedés
- A jogos védelemnél az elhárítás szükséges mértékének túllépése [Btk. 22. § (3) bek.]
- A végszükségnél az elhárítás szükséges mértékének túllépése [Btk. 23. § (2) bek.]
- Az elöljáró parancsa

Büntethetőséget megszüntető okok:

- Az elkövető halála
- Az elévülés

[5] Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017.

– A kegyelem
– A tevékeny megbánás
– A törvényben meghatározott egyéb ok

A büntetőjogi felelősségre vonás egyéb akadályai:

– A magánindítvány hiánya
– A feljelentés hiánya
– A törvényben meghatározott további okok

A büntethetőséget kizáró (korlátozó) körülményeket tudományos szempontból alapvetően azon ismérv alapján lehet csoportosítani, hogy a bűncselekmény mely fogalmi elemét küszöbölik ki. Miután a Btk. 15. §-ában felsorolt egyes körülmények a jogellenességet, mások a bűnösséget zárhatják ki, célszerű különbséget tenni jogellenességet, valamint bűnösséget kizáró okok között. A jogellenességet kizáró okok alapvetően objektív, míg a bűnösséget kizáró körülmények szubjektív színezetű tényezőknek tekinthetőek.

A büntethetőséget objektív alapon zárja ki a jogos védelem alapesete [Btk. 22. § (1) bek.], a végszükség alapesete [Btk. 23. § (1) bek.] és a jogszabály engedélye (Btk. 24. §). Szubjektív alapon, tehát az elkövető tudatában, illetve akaratában rejlő kizáró körülmény a gyermekkor, a (kizáró jellegű) kóros elmeállapot, a kényszer és fenyegetés, a tévedés (hacsak nem gondatlanság okozza), valamint a jogos védelem és a végszükség szükséges mértékének exkulpatív értékelése [Btk. 21. § (3) bek.; 23. § (2) bek.]. A korlátozott beszámítási képesség – akár kóros elmeállapot, akár kényszer, illetve fenyegetés esetén [Btk. 17. § (2) bek., 19. § (2) bek.] – felelősséget csökkentő büntetéskiszabási szabálynak tekintendő ebben a rendszerben.

Az Általános Részben – a Btk. 15., 25. és 30. §-aiban okok nem merítik ki teljesen a büntethetőségi akadályok körét. A Btk. 15. § h) pontja, illetve a 25. § e) pontja szerint a törvény meghatároz olyan körülményeket, melyek az Általános Rész más helyén vagy éppen a Különös Részben elhelyezkedve ugyanolyan hatással bírnak, mint az említett Btk. 15. és 25. §-aiban meghatározott okok.[6] Ezeken túlmenően számos büntethetőséget kizáró okot a joggyakorlat a tudománnyal karöltve dolgozott ki (pl. sértett beleegyezése).

A jogellenességet kizáró okok rendszere tágabb körű, mint a Btk. Általános és Különös Részében nevesített okok köre. Ebbe a körbe a részben bírói gyakorlatban

[6] Itt emelhető ki, hogy egy hasonló „egyéb" kategóriára a törvényi egyértelműség és a dogmatikai tisztaság érdekében a 30. §-ban is szükség lenne, hiszen itt is vannak olyan további büntethetőségi akadályok (pl. a legfőbb ügyész döntésének a hiánya a büntetőeljárás megindításáról), amelyek dogmatikai természete a magánindítvány és a feljelentés hiányával azonos.

kialakult és a jogirodalomban nevesített jogellenességet kizárók okokat soroljuk. Ezek nem törvény feletti jogellenességet kizáró okok, a büntetlenség kifejezetten a Btk. rendelkezésén alapul. A Btk. 4. § (2) bekezdésében ugyanis az jut kifejezésre, hogy az olyan cselekmény, amely nem sérti és nem is veszélyezteti a jogi tárgyat, bűncselekménynek nem tekinthető (kivétel az alkalmatlan kísérlet egyes esetei). Ide soroljuk a sértett beleegyezését, a fegyelmezési jog gyakorlását, az indokolt (megengedett) kockázatot, valamint a hivatás gyakorlását.

Az alábbiakban nem valamennyi, csupán azon büntethetőségi akadályokat veszszük szemügyre közelebbről, amelyek prekoncepciónk szerint az autonóm járművek kapcsán relevanciához juthatnak.

3. A jogellenességet kizáró okok

Jogellenességet kizáró ok fennforgása esetén a cselekmény nem büntetendő, így annak kapcsán büntetőjogi felelősség egyáltalán nem – más személy kapcsolódó magatartása viszonylatában sem – állapítható meg. A bűnösséget kizáró okokkal szemben tehát alapvetően objektív természetű büntethetőségi akadályról beszélhetünk ebben az esetben.

3.1. A jogos védelem

A jogos védelem az elsődleges büntethetőségi akadályok között, részben a (materiális) jogellenességet [más megnevezéssel társadalomra veszélyességet; Btk. 22. § (1) bek.], részben pedig a bűnösséget kizáró okok közé tartozik [Btk. 22. § (3) bek.]. Jogos védelem alatt tradicionálisan a 22. § (1) bekezdésében szabályozott kizáró okot értjük, így először azt vizsgáljuk (klasszikus jogos védelem). Ugyanakkor jelezhető, hogy az utóbbi évek büntető-jogalkotásában a jogintézmény erőteljes expanziója volt megfigyelhető, melynek keretében a klasszikus jogos védelmi szabályok mellett a törvényhozó ma már a megelőző jogos védelem (Btk. 21. §), valamint a szituációs jogos védelem szabályait [Btk. 22. § (2) bek.] is megjeleníteni. Szintén rögzítendő, hogy az Alaptörvény V. cikke szerint: „[m]indenkinek joga van törvényben meghatározottak szerint a személye, illetve a tulajdona ellen intézett vagy az ezeket közvetlenül fenyegető jogtalan támadás elhárításához". Eme alkotmányos jogosultság ugyanakkor csupán a jogos önvédelem lehetőségét biztosítja, a mások vagy a közérdek védelmében történő fellépés lehetősége explicit alapjogként nem került megjelenítésre. A jogos védelem egyébként nem büntetőjog-specifikus intézmény, hiszen például a Ptk. 6:520. § b) pontja is kimondta, hogy „[m]inden károkozás jogellenes, kivéve, ha a károkozó a kárt a jogtalan támadás vagy a jogtalan és közvetlen támadásra

utaló fenyegetés elhárítás érdekében a támadónak okozta, ha az elhárítással a szükséges mértéket nem lépi túl". E fogalmazásból kitűnően ugyanakkor a büntetőjogi jogos védelem lényegesen tágabb térfogatú a kárfelelősség kapcsán olvasható polgári jogi társánál, ezért a gyakorlatban előbbi jut nagyobb jelentőséghez.[7]

A jogos védelem büntetőpolitikája egyrészt a megtámadott, védekező személy társadalom erkölcsi normáiból és az állam büntetőhatalmából, másrészt pedig a „természetjog" által biztosított önvédelemhez való jogból ered.

Ami a jogos védelemnek az autonóm járművek kapcsán felmerülő kérdéseit illeti, kiemelhető, hogy a valódi világban, ahol az Asimov 'Robotika törvényei' nem léteznek, a robotok veszélyt jelenthetnek az életre, a tulajdonra és az ember magánéletére nézve is. Így felmerülhetnek olyan kérdések, mint amilyen az, hogy feltétlenül elkerülje-e a járműben ülő személyek sérülését az autonóm jármű?

Az egyesült államokbeli Froomkin és Colangelo szerzőpáros véleménye szerint az autonóm járművek kapcsán tehát természetszerűen vethető fel az élet és a testi épség fizikai sérelme. Így a Google Térkép révén balesetet idézhet elő a gyalogost elgázoló önvezető autó; de hasonló példa, hogy az Amazon által küldött drón egy csomagot dobhat a sértett fejére. Az autonóm robotok fizikai fenyegetést is jelentenek a tulajdonra, sérthetik a kizárólagos birtokláshoz való jogot. Ezért például a már említett Google Térképnek is biztosítania kell(ene) a félrevezető információk kiszűrését. Végül az autonóm robotok veszélyt jelentenek a magánéletre is. Így könnyedén kémkedhetnek, információt rögzíthetnek vagy lehallgathatnak olyan helyzetekben, ahol ugyanez az ember számára lényegében lehetetlen lenne. A vezető nélküli autók speciális problémákat vetnek fel, mert nem csupán KRESZ-szabályszegések potenciális lehetőségét, hanem akár közlekedési bűncselekmények káros eredményének megvalósulását is magukban hordozhatják.[8]

Ami e vonatkozásban a jogos védelem hazai megítélését illeti, kiemelendő, hogy e jogellenességet kizáró ok hatályosulásának elementáris feltétele, hogy az önvezető jármű ne a betáplált – majd az okos-technológiára figyelemmel időközben magába épített – információk alapján idézzen elő sérülést vagy legalább veszélyhelyzetet. Ehelyett jogos védelemről – miután annak feltétele a jogtalan támadás – kizárólag abban az esetben beszélhetünk, amikor az önvezető jármű eszközként szerepel egy természetes személy elkövető kezében. Így, ha például a hackertámadás célja

[7] A BH 1980. 128. kifejezetten utal arra, hogy „[a] jogos védelem polgári jogi fogalma és a büntetőjogi fogalom nem szükségképpen esik egybe. A büntetőjogi megoldással ellentétben a polgári jog nem biztosít kifejezett mentességet annak, aki a jogos védelem határait ijedtségből vagy felindulásból túllépte".

[8] Froomkin, A. Michael – Colangelo, P. Zak: Self-Defense Against Robots and Drones. Connecticut Law Review 2015/1. 7. o.

a sértett megölése, az önvezető járműnek az erre történő beprogramozása ugyanúgy (büntetőjogi értelemben vett) cselekménynek tekinthető, mintha az elkövető például egyszerűen egy lőfegyverrel vagy szúró-vágó eszközzel próbálna végezni a sértettel. Még inkább rokonítható lehet ez a megoldás az állat uszításával elkövetett testi sértési és emberölési cselekményekkel. Az állat ilyenkor saját maga – mivel sem magánjogi értelemben nem jogalany, sem büntetőjogilag nem tekinthető a bűncselekmény alanyának – jogtalan támadást nem tud megvalósítani.[9] Arra azonban alkalmas, hogy az ember jogtalan támadásához eszközként szolgáljon. Ezért ezen felfogást lehetne érvényre juttatni akár az ember által, sértő eredmény előidézése érdekében felhasznált autonóm jármű esetében is.

3.2. A végszükség

A Btk. 23. § (1) bekezdésében szabályozott végszükség ugyancsak jogellenességet, míg a túllépésére vonatkozó (2) bekezdés valójában bűnösséget kizáró ok. A végszükségi a jogos védelmi helyzettel megegyezik abban, hogy itt is egy külső, hátránnyal fenyegető helyzetet háríthat el az e jogával élő személy, különbség viszont az, hogy a végszükség nem harmadik személy jogtalan támadása folytán következik be. Kialakulása a törvényben nincs rögzítve, viszont a jogos védelemtől és a kényszer és fenyegetéstől való elhatárolás során kiviláglik, hogy vagy embertől független okfolyamat hozza létre e veszélyhelyzetet (árvíz, villámcsapás okozta tűzvész, tűzhányó kitörés stb.), vagy pedig olyan okfolyamat, amely bár emberhez köthető, mégis annak a személynek, aki azt elindítja, „támadása" nem jogellenes (maga is végszükségben cselekszik).[10] Amennyiben ugyanis jogellenes támadás következtében jön létre a veszélyhelyzet, úgy az elhárító cselekményt a jogos védelem szabályai szerint kell elbírálni. Az emberi támadás jogossága, és hogy hiányzik a materiális jogellenesség (társadalomra veszélyesség) a támadó oldalán alapozza meg az elhárító magatartás mértéke közötti különbséget e két hasonló jogintézmény között: a jogos védelem esetében a szükséges mérték, míg végszüksége esetén a kisebb sérelem a mérce.

A végszükség problémaköre kapcsán az önvezető járművek viszonylatában valószínűleg a leghíresebb, ún. „villamos-dilemma" kérdésköre vethető fel. Az önvezető technológia megjelenésével ugyanis a programozóknak az alkalmazott etika kérdésében is szükséges döntést hozniuk, amelyben a modern filozófia, pszichológia és jogszociológia bevonása is elengedhetetlen. A kérdést számos formában feltették

[9] A legújabb kúriai gyakorlatból lásd EBH 2018. B. 24.

[10] A keletkeztető okokhoz az angol jogirodalomban lásd Bohlander, Michael: Of Shipwrecked Sailors, Unborn Children, Conjoined Twins and Hijacked Airplanes – Taking Human Life and the Defence of Necessity. The Journal of Criminal Law 2006/2. 147-161. o.

már, amely egyik legszemléletesebb megfogalmazása Noah Goodall nevéhez fűződik. Ezt később Patrick Lin tovább pontosította. A tényállás és a kérdés röviden: „Egy önvezető autó egy elkerülhetetlen ütközés előtt áll. Két irányba módosíthatja irányát, az egyik esetben egy sisakot viselő motorost üt el, a másik esetben egy sisak nélkülit. Mi a helyes megoldás?"[11]

A kérdés azonban tovább fokozható; az ugyanúgy Lin nevéhez fűződő dilemma[12] szerint az egy személyt szállító, teljesen önvezető autó érzékeli, hogy vagy egyenesen belehajthat egy 28 gyermekkel utazó iskolabuszba, így kockáztatva mindenki életét, vagy a haladási irányt megváltoztatva egy szakadékba hajthat, amely az adott személy biztos halálával járna. Amennyiben az ütközés során minden személy ugyanolyan eséllyel éli túl, kérdés, hogy a mesterséges intelligencia kialakítása milyen irányú legyen; minden esetben kockáztasson, vagy ne vállaljon rizikót és hajtson bele a szakadékba (amely a benne ülő halálával járna), esetleg végezzen gyors kalkulációt, és csak akkor hajtson a szakadékba, ha 1:30-nál nagyobb eséllyel szenved valaki halálos sérülést az ütközés során?

Az egyébként nem újkeletű kérdésre egyértelmű, mindenki számára elfogadható válasz nem adható, csupán érvelni lehet az egyes válaszok helyessége mellett. Az etikai kérdések egyik kiindulópontja a számtalanszor feltett villamos-dilemma – a szcenárióban egy vasúti sínen öt gyanútlan ember áll (egyes verziókban öt figyelmetlen munkás dolgozik), egy másik vágányon pedig egy. A vonat megállíthatlanul száguld az öt felé, a pályakezelő pedig dönthet – eltérítse a vágányt, ezzel (szinte biztosan) az egyedül dolgozó munkás halálát okozva, ha ezzel megmenti az eredeti úton dolgozó öt másikat? A hipotézis szerint a kérdésre adott válaszokból kikövetkeztethető a társadalmi morál, amely így a gyakorlatba is átültethető.[13]

Ami a végszükség hatályos szabályozása alapján történő megítélést illeti, a feltétlen büntetlenséghez legfeljebb akkora sérelmet lehet okozni, amekkorával a közvetlen és másként el nem hárítható veszélyhelyzet fenyeget. Ez tehát azt jelenti, hogy amennyiben az önvezető jármű haladása kapcsán felmerülő baleseti szituáció egy emberélet sérelmével fenyeget, a végszükség keretébe tartozhat a járműben helyet foglaló – utas, emberi operátor vagy tesztvezető – legalább egy, de akár több személy életének megmentése. Ezzel szemben, ha a baleset egynél több (legalább kettő) gya-

[11] Lin, Patrick et al.: From Autonomous Cars to Artificial Intelligence, Oxford University Press. Oxford, 2017. 21. o.

[12] Lin, Patrick: Why Ethics Matters for Autonomous Cars. In: Maurer, Markus et al. (ed.): Autonomous Driving. Technical, Legal and Social Aspects, Springer Open, 2016. https://link.springer.com/content/pdf/10.1007%2F978-3-662-48847-8.pdf, 76. o. [2018.12.14.]

[13] Greene, Joshua D.: Solving the Trolley Problem. In: Sytsma, Justin – Buckwalter, Wesley (ed.): A Companion to Experimental Philosophy. John Wiley & Sons, Ltd. Chichester, 2016. 175. o.

logos életét fenyegeti, a járműban azonban csak egy (avagy a gyalogosok számánál mindig legalább eggyel kevesebb) személy foglal helyet, a végszükségre – legalábbis annak jogellenességet kizáró alapesetére – eredményesen hivatkozni nem lehet.

Itt indokolt kiemelni, hogy Magyarország Alaptörvényének XV. cikk (2) bekezdése értelmében „Magyarország az alapvető jogokat mindenkinek bármely megkülönböztetés, nevezetesen faj, szín, nem, fogyatékosság, nyelv, vallás, politikai vagy más vélemény, nemzeti vagy társadalmi származás, vagyoni, születési vagy egyéb helyzet szerinti különbségtétel nélkül biztosítja". Röviden tehát valamennyi ember élete egyenértékű. Így alkotmányos szempontból sem fogadható el az önvezető jármű olyan formában történő programozása, amelynek alapján az például előnyben részesítené a fiatalok életét az idősekével, a férfiakét a nőékkel (vagy fordítva), az egészséges személy életét a rokkantéval, stb. Itt tehát jelentőség érdekösszeütközés is fel fog tudni merülni, ami nemcsak – sőt nem elsősorban – büntetőjogi, hanem alapvetően morális, társadalmi kérdésként fog jelentkezni és vár mielőbbi megválaszolásra.

Végül Thomas Weigend kölni professzor legújabb vonatkozó álláspontját érdemes a végszükség problémaköre kapcsán kiemelni, amelynek értelmében az önhajtású autók programozására vonatkozó az alábbi szabályok megtartása mellett lehetnek a lehető legkevésbé aggályosok:

Ha a balesettel fenyegető helyzetben mindössze azon választás lehetősége létezik, hogy kisebb vagy nagyobb számú emberrel ütköznek (végzetes következményekkel), akkor a kisebb számmal kecsegtető ütközést kell kiválasztani. Ez Weigend szerint akkor is érvényes, ha ütközés hatással van a jármű utasaira. Ha azonban csak azon lehetőségek közül választhat az autonóm jármű programja, hogy összeütközésbe kerül emberek több csoportja (halálos következményekkel), akkor a véletlennek kell eldöntenie a jármű útját. Ugyanakkor, ha az érintett csoportok valamelyike a jármű utasai, akkor azt kell választani, amely lehetőség szerint a járműben ülőket megmentheti.[14]

3.3. A megengedett (indokolt) kockázat

A WHO adatai szerint az egész világon 2013-ban pedig több mint 1,2 millió ember halt meg közlekedési balesetekben, ez a vezető halálozási ok a 15-29 éves korosztályon belül.[15] Ami pedig a hazai vonatkozásokat illeti, Magyarországon, a KSH adatai szerint 2016-ban 16.627 közlekedési baleset végződött személyi sérüléssel, amelyek

[14] Weigend, Thomas: Notstandsrecht für selbstfahrende Autos? Zeitschrift für Internationale Strafrechtsdogmatik 2017/10. 605. o.

[15] WHO Global Status Report on Road Safety, WHO Press, Genf, 2015. http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/ [2018.12.14.]

során 607-en vesztették életüket, és 21.239-en sérültek meg. A baleseteket legtöbbször, 15.247 esetben a járművezetők idézték elő, ezt a második legnagyobb gyakorisággal a gyalogosok követik (961 alkalom). A járművekben jelentkező műszaki ok mindössze 81 alkalommal okozott balesetet, míg pályahibák és egyéb okok 210 alkalommal. Ez alapján elmondható, hogy összesen csupán 2%-ban okozta nem emberi tényező a baleseteket, az összes baleset 91%-áért pedig a vezetők tehetők felelőssé.[16]

Egy frissen publikált tanulmány szerint ugyanakkor például az USA-ban átlagosnak tekinthető évi 41.000 közlekedési haláleset kb. legfeljebb 200-ra lenne csökkenthető az önvezető járművek (ezen belül: autók és akár kamionok) elterjedésével.[17] Ha a cikkben említett arányszámot Magyarország 600 körüli halálozási számára vetítjük, évi körülbelül 3, míg világszinten kevesebb mint 6000 halálokozást jelentene. Természetesen az említett adat közel sem tekinthető pontosnak, hiszen a világszerte történő elterjedésre óvatos becslések szerint évtizedeket is várni kell még, valamint az is várható, hogy az önvezető és a nem önvezető járművek hosszú időn keresztül egymás mellett fognak élni. A technika várható fejlődése mellett ugyanakkor az önvezető járművek révén a közlekedési balesetek és halálesetek exponenciális csökkenése prognosztizálható. Ebből pedig a büntetőjogi értékelés számára a következő dilemma merül fel. Amennyiben az autonóm járművek nyomán lényegesen csökken a sértő eredménnyel járó balesetek (és ekként általában közlekedési deliktumok) száma, a büntetőjog ultima ratio jellegére is figyelemmel, beleférhet-e a megengedett kockázat mint jogellenességet kizáró ok fogalomkörébe, hogy büntetlenül maradjanak azok az ugyanilyen eredményt előidéző balesetek, amelyeket a jövőben az önvezető járművek okoznak?

E kérdés megalapozott megválaszolásához a büntetőjog alapjogi, valamint emberi jogi korlátaiból érdemes kiindulni. Magyarország Alaptörvényének II. cikke szerint minden embernek joga van az élethez és az emberi méltósághoz. Az Emberi Jogok Európai Egyezményének 2. – utóbb a 7. kiegészítő jegyzőkönyvvel megszorított tartalmú – cikke szerint sem lehet senkit életétől szándékosan megfosztani. Az élethez való jog tehát csak kivételesen, pontosan meghatározott törvényes keretek között lehet korlátozni (nullum crimen sine lege), amire például szolgálhat a jogos védelem intézménye (Btk. 21-22. §). Szokásjogi úton érvényesülő jogellenességet kizáró ok

[16] KSH: Közlekedési balesetek 2017. http://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_ods001.html [2018.12.14.];

Az adatokat részletesen elemzi Hodula Máté: Az önvezető járművek és a büntetőjogi felelősség. Jogelméleti Szemle, 2018/3. 68-78. o.

[17] End of the road. Will automation put an end to the American trucker? https://www.theguardian.com/technology/2017/oct/10/american-trucker-automation-jobs [2018.12.01.]

(mint amilyen az indokolt kockázat mellett a sértett beleegyezése, a fegyelmezési jog, valamint a hivatás gyakorlása) alapján azonban az emberi élet nem oltható ki. Így például a sértett beleegyezése körében a könnyű testi sértésbe történő beleegyezés tekinthető csak csupán joghatályosnak, a fegyelmezési jog kapcsán pedig még ennek is kevesebb, legfeljebb a tettleges becsületsértés „férhet bele" a szülő részéről. Érdekes kérdéseket vet fel például az orvosi hivatás gyakorlása körében okozott sérelem (pl. műhiba), amely körében akár halálos eredmény is bekövetkezhet, ez azonban sem szándékos, sem gondatlan nem lehet, hanem az orvosi hivatásra vonatkozó szabályok maradéktalan betartása melletti sérelemokozásról lehet csupán szó.[18] Mindezek alapján a megengedett kockázat keretében történő halálokozás csak de lege ferenda, ilyen irányú, kifejezett törvényi rendelkezés megteremtése mellett foghatna helyt, jelenlegi jogszabályi berendezkedésünk keretei között nem.[19] Ugyanez lehet a helyzet a könnyű, legfeljebb 8 napon belül gyógyuló testi sérülésnél súlyosabb sérelem (pl. súlyos testi sértés, maradandó fogyatékosság, életveszély, stb.) esetében is.

Némileg más megítélést igényelhetnek az alapesetben materiális veszélyeztető, valamint az absztrakt veszélyeztető (tehát immateriális) közlekedési bűncselekmények. Előbbieket az jellemzi, hogy sérülés nem, csupán (közvetett vagy közvetlen) veszély következik be az elkövető szabályszegő magatartásával okozati összefüggésben (pl. közúti veszélyeztetés). Utóbbiaknál pedig sem sérelem, sem veszély nem szükséges a bűncselekmény befejezetté válásához, az elkövetési magatartás azonban potenciálisan ezek létrehozatalára alkalmas (ilyen a már említett ittas, de ugyanígy a bódult állapotban történő járművezetés is).

A jogellenességet kizáró ok szokásjogi (tehát bírói vagy ügyészi) úton történő tágítása a normavilágosság követelményével kevésbé fér össze, ezért ebben a körben inkább jogalkotói lépések szükségessége merülhet majd fel. Az említett jellegű deliktumok vonatkozásában ugyanis már felvethető, hogy a büntetőjog ultima ratio jellege büntetési tételeik mérséklése, majd a későbbiekben esetlegesen akár dekriminalizációjuk megfontolása mellett szól, hiszen nagyobb társadalmi előny várható az önvezető járművek elterjedéséből fakadó csökkenő számú balesettől, mint attól, hogy a felmerülő, várhatóan egyre csekélyebb számú elkövetőket a jelenlegi tényállások és büntetési tételek alapján, feltétlenül felelősségre vonjuk. Emellett a legfeljebb súlyos testi sérülést okozó, ugyanakkor gondatlanságból elkövetett közlekedési bűncselekmények (ilyen alapesetben a közúti baleset okozása, de más közlekedési deliktumoknak is van gondatlan alakzata) viszonylatában is megfontolandó lehet a büntetőjogi felelősség mérséklése, vagy akár a büntetőjogi úttól való eltekintés.

[18] Gellér – Ambrus: i.m. 252-261. o.

[19] Ennek lehetősége természetesen csak gondatlan halálokozás kapcsán vethető fel egyáltalán.

Utóbbira egyébként már most is van példa, hiszen a közúti baleset okozása kapcsán például helye lehet a tevékeny megbánás (Btk. 29. §) útján a büntethetőség megszűnésének, jóllehet ezen deliktum alapesetben is súlyos testi sérüléssel jár.

A legmegnyugtatóbb megoldás tehát mindenképpen a kifejezett törvényi szabályozás lenne a szokásjogi úton történő felelősség-eliminálás helyett. Ennek egyik módja a Btk. Általános Részében – vagy más jogági norma[20] – megfelelő, részletes szabályozásának megteremtése lenne, például a megengedett kockázat részletszabályainak törvényi megjelenítése révén. Emellett elképzelhető, hogy a jelenleg materiális vagy absztrakt veszélyeztető tényállásokat materiális sértő deliktumokká kerüljenek törvényhozói átalakításra. Megfontolásra érdemes lehet továbbá a járművezetés ittas állapotban (Btk. 236. §) bűncselekménye kapcsán az ittasság büntetőjogi fogalmában [Btk. 240. § (3) bek.] újragondolása is.[21] A büntetőjog ultima ratio jellege ugyanis a végső esetben, utolsó eszközként való büntetőjog-alkalmazás lehetővé tételét kívánja meg a jogalkotótól. E kívánalomnak pedig önvezető járművek által okozott, büntetőjogilag releváns eredmények viszonylatában várhatóan csak akkor felel majd meg, ha az autonóm járművek által képviselt új technológiai innovációnak nagyobb teret enged, akár az állam büntetőhatalmának érvényesítési körének szűkítése révén is. Ellenkező esetben a technikai fejlesztések visszaesésével is lehet számolni, amely kontraproduktív következmény lenne, hiszen végeredményben több sérüléssel és halálokozással járhat, mint a jelenleginél megengedőbb, a veszélyeztető deliktum-konstrukciók miatti büntetőjogi szankciók mértékét enyhítő, vagy azokat akár ki is iktató esetleges jövőbeli szabályozás.

4. A bűnösséget kizáró okok

A bűnösséget kizáró okok alapvetően szubjektív természetű elsődleges büntethetőségi akadályok, tehát nem a megvalósult cselekményhez, hanem szorosan az elkövető személyéhez tapadnak. Ezért az ilyen körülményeket szabályozó rendelkezések nem a cselekmény büntetendőségének, hanem az elkövető büntethetőségének a hiányáról rendelkeznek. Témánk szempontjából a kóros elmeállapot mint bűnösséget kizáró ok alkalmazását lehetetlenítő ittas vagy bódult állapotban elkövetett bűncselekmény, valamint a tévedés témakörét érdemes felvetni.

[20] A keretdiszpozíciós megoldás is tökéletesen megfelelne a nullum crimen sine lege elvének, hiszen a hatályos Btk. 24. §-a, tehát a jogszabály engedélye révén közvetlenül hatályosulhatna a büntető jogalkalmazásban.

[21] E kérdéskör önálló, részletes körüljárást fog igényelni.

4.1. Az ittas vagy bódult állapotban elkövetett bűncselekmény

A Btk. 17. § (1) bekezdése szerinti kóros elmeállapot az elkövető bűnösségének, ezen belül a beszámítási képességének hiányát eredményezi. A bűnösség tudati, akarati és érzelmi oldalból tevődik össze. A felismerési képesség a cselekmény következményeinek előrelátására, valamint a cselekmény társadalomra veszélyességének felismerésére való képesség. Az akarati képesség az akarat képzésére és az akaratnak megfelelő magatartás tanúsítására való képességet jelenti. A bűnösség tudati, akarati oldalát érinti az elkövető beszámítási képességének a hiánya, azaz ezen ok is beszámítási képességet kizáró ok.[22] A kóros elmeállapot egyik esete a tudatzavar.

A tudatzavar egy olyan átmeneti állapot, amelyben a tudat elhomályosul, beszűkül. A tudatzavart embernek mind a saját személyéről, mind a külvilágról csupán hiányos, homályos képzete van, illetve öntudatlan állapot esetén semmilyen. Tudatzavart állapotot számos ok idézhet elő így különösen különböző idegmérgek, kábítószerek, alkohol, rendkívüli megrázkódtatás, kimerültség, de keringési zavarok, cukorbetegség is. A különböző indulatok által kiváltott cselekmények kapcsán leszögezendő, hogy csak a kóros, ún. pathológiás indulat zárja ki a büntethetőséget, az éplélektani alapon kialakuló ún. fiziológiás indulat talaján kialakuló rövidzárlati cselekmény esetében nincs mód a 17. § alkalmazására.

Az ittas vagy bódult állapot az elmeműködés szempontjából a tudatzavar egy speciális esetének minősül, a beszámítási képesség ebben az állapotban is korlátozott, illetve kizárt. Ezért elméletileg az ittas vagy bódult állapotú elkövető bűnössége sem áll fenn. Azonban büntetőpolitikai szempontok miatt megengedhetetlen lenne, hogy az ittas vagy bódult állapotban lévő elkövető ne legyen büntethető cselekményéért.

Hatályos jogunk úgy rendelkezik, hogy az önhibájából ittas vagy bódult állapotban lévő elkövető cselekményét úgy kell elbírálni, mintha az elkövető rendelkezett volna beszámítási képességgel, és felelősségre kell vonni azért a bűncselekményért, amit elkövetett.[23] A 18. § tehát kategorikusan kizárja a kóros elmeállapotra vonatkozó szabályok alkalmazását ebben az esetkörben.

A törvény szerint a kóros elmeállapot mint büntethetőséget kizáró ok, alkalmazása tehát akkor tilos, ha az ittas vagy bódult állapot az elkövető önhibájából ered. Tulajdonképpen az önhiba teremti meg a hiányzó szubjektív oldalt, hiszen amikor az elkövető az ivást elkezdte, tisztában volt az ital vagy a bódító szer hatásával. Az it-

[22] Vö. 3/1998. BJE

[23] Lásd Berkes György: Az ittas állapotban elkövetett bűntett jellege. Magyar Jog, 1965/2. 56-60. o., Somogyi Zoltán: A bódult vagy ittas állapotban elkövetett bűncselekményekért való felelősség. Collega, 2005/2. 94-97. o.

tas, vagy bódult állapotban elkövetett cselekményért való felelősség eltér a bűnösség általános alakjától, tulajdonképpen egyfajta közvetett tudat létezik, nem a konkrét bűncselekmény elkövetésére, hanem a lerészegedésre nézve. A beszámítási képességet kizáró ittas vagy bódult állapotban elkövetett cselekményért való felelősség tehát valójában tárgyi (objektív) felelősség. Az elkövető ugyanis nem a leittasodásért, vagy a bódult állapot előidézéséért tartozik felelősséggel (ezekre kiterjed az „önhibája"), hanem azért a többnyire szándékosan elkövetettnek tekintendő cselekményért, amelyre nézve általában még ún. határozatlan gondatlanság sem terheli. Az alanyi oldalnak a Btk. 18. §-án alapuló felelősségnél is jelentősége van, de csupán az önhibából eredő leittasodás, nem pedig az ittas állapotban elkövetett bűncselekmény konkrét tényállása vonatkozásában. A bíróságnak ennyiben kell az alanyi oldalt vizsgálnia. Azt kell tehát vizsgálnia, hogy a terheltnek a tudatzavart előidéző leittasodása önhibából eredt-e. A bűncselekménnyel kapcsolatos értelmi-érzelmi viszonyulás nem bűnösségi feltétel.

Kérdésként jelentkezik, hogy az ittas (és kisebb éllel ugyan, de a bódult állapotban) elkövetett cselekmény megítélése változni fog vagy változatlanul marad az önvezető járművek elterjedése esetén. Nem elképzelhetetlen ugyanis, hogy a hazánkban jelenleg irányadó zéró tolerancia-elv enyhítést fog igényelni az ittas járművezetés viszonylatában, mivel nagyobb társadalmi érdek fűződik ahhoz, hogy a megfelelően programozott és rendeltetésszerűen közlekedő autonóm járművek utasai/emberi operátorai adott esetben bizonyos mennyiségű szeszesitalt fogyasztó személyek is lehessenek a jövőben, mint ahhoz, hogy feltétlenül fenntartsuk a legminimálisabb alkoholfogyasztást sem toleráló jelenlegi szabályozást.

Az Egyesült Államokbeli szakirodalomban KATHERINE L. HANNA mutatott rá arra, hogy az ittas vagy bódult állapotban történő vezetés komoly közegészségügyi aggodalomra ad okot. Egyes becslések szerint 112 millió alkoholfogyasztással együtt járó vezetésre kerül sor az Egyesült Államokban a felnőttek körében évente. 2012-ben 10 322 embert halt meg az alkohollal kapcsolatos közúti balesetben. Ez a közlekedési balesetek közel egyharmadát tette ki az Államokban, amely alapján átlagosan 51 percenként történt egy-egy haláleset. Nem csak az ittas vagy bódult vezetés befolyásolja az érintett személyek egészségét és biztonságát, ez szintén óriási gazdasági terhet ró az adófizetőkre. 2010-ben, több mint 1,4 millió amerikai embert tartóztattak le alkohol vagy bódító hatású szer miatti vezetés miatt. Továbbá az alkoholfogyasztás és a kábítószer-fogyasztással megvalósított vezetés pénzbe kerül a bűnüldözés, a bíróságok, a börtönök, a munkából kiesett idő, sérülések, vagyoni károk és a halálesetek miatt is. Becslések szerint csak 2009-ben, az ittas vezetések költsége az USA adófizetői számára 132 milliárd dollárba került. Mindezen indokok alapján az idézett szerző a következő javaslatokat teszi. Felvázolható jogalkotási

alternatíva az, hogy ne büntessük azokat az ittas/bódult személyeket, akik biztonságosan a járművel az út szélére húzódnak, ha az autonóm jármű működése kapcsán üzemzavart érzékelnek. E vonatkozásban Washington állam jelenleg olyan szabályozással rendelkezik, amely tiltja az ittas vezetők büntetését, akik biztonságosan az út szélére húzódnak olyankor is, ha túlzott fokú ittasságukat észlelik. Ez azonban megoldás azonban a szerzői álláspont szerint várhatóan nem fogja elrettenteni az önvezető járművek üzemeltetésétől az ittas személyeket, figyelemmel arra, hogy ittas állapotban az emberek nagyobb valószínűséggel vállalkozhatnak kockázatos cselekményekre. Az ittas személyek ugyanis gyakran, közismert módon, irracionálisan viselkedik, és azt hiszik, hogy nincsenek az alkohol hatása alatt. Ha azonban az önvezető jármű ilyenkor beavatkozást igényel, az ittas személy jó eséllyel passzív maradhat. Egy lehetséges megoldás az autonóm jármű gyártói a járműveiket gyújtáskapcsoló (az alkoholfogyasztás mértékét érzékelő) eszközökkel felszereljék. Ilyen esetben, ha a járműben helyet foglaló személy ittasságának (bódultságának) szintje meghalad egy bizonyos küszöbértéket, a járművet irányításának jogát megvonná az ittas/bódult személytől, és a járművel haladéktalanul az út szélére húzódna.[24]

4.2. A tévedés

A tévedés a szándékos bűnösség tudati oldalának fogyatékosságát jelenti, így bűnösséget kizáró ok. A tévedés az elkövető tudatában valónak és valótlannak a felcserélése, aminek következtében a tévedésben lévő elkövető nem olyan magatartást tanúsít, mint amilyet a valóság ismeretében tanúsítana. A tévedés tárgyát tekintve a törvény megkülönböztet ténybeli és társadalomra veszélyességben való tévedést, de a jogtudomány vizsgálja a jogban való tévedést is.

A ténybeli tévedés a törvényi tényállás tárgyi oldalának valamelyik elemében való tévedést jelenti. A szándékos bűnösség ugyanis csak akkor áll fenn, ha az elkövető tudata átfogja a bűncselekmény törvényi tényállásának tárgyi ismérveit. A ténybeli tévedés csak akkor minősül relevánsnak, ha olyan tényre vonatkozik, amire a szándékosságnak ki kell terjednie [kivéve persze a Btk. 20. § (3) bekezdését]. Amennyiben ugyanis a tévedést gondatlanság okozza, és az adott bűncselekménynek gondatlan változatát is szabályozza a törvény, a felelősség emiatt megállapítható.

A tévedésre történő hivatkozás alapvetően akkor jöhetne szóba, ha az autonóm jármű által gyűjtött és a további mozgás szempontjából determinálónak bizonyuló információ tartalmával az emberi operátor nincs tisztában. Így ha például a Google Térkép üzemzavar miatt végül tévesnek bizonyuló információkat szolgáltat, a

[24] Hanna, Katherine L.: Old Laws, New Tricks: Drunk Driving and Autonomous Vehicles. Jurimetrics 2015/3. 288. o.

büntetőjogi felelősség kizárható válik. Ugyanez lehet a helyzet, ha az elkövető személyétől független ok – például a vezeték nélküli internetkapcsolat megszakadása – idézi elő az autonóm jármű által kiváltott balesetet.[25]

5. Összegzés

Az önvezető járművek kapcsán számtalan bűncselekménytani problémakör felvethető. Ezek közül alapvetően azok jutnak majd várhatóan determináló jelentőséghez, amely a büntetőjogi felelősség enyhítését vagy eliminálását vonhatják maguk után, valamint azok az esetek, amelyek a közvetlenül cselekvőnek tekinthető személyhez képest egy másik – mögöttes – személy büntetőjogi felelősségének kérdését vetik fel. Mindezen tapasztalatok akár évszázadok óta rögzült dogmatikai nézetek felülvizsgálatának szükségességét is megalapozhatják és indokolhatják.

Felhasznált irodalom

Berkes György: Az ittas állapotban elkövetett bűntett jellege. Magyar Jog, 1965/2.

Bohlander, Michael: Of Shipwrecked Sailors, Unborn Children, Conjoined Twins and Hijacked Airplanes – Taking Human Life and the Defence of Necessity. The Journal of Criminal Law 2006/2.

Brożek, Bartosz – Jakubiec, Marek: On the legal responsibility of autonomous machines. Artifical Intelligence and Law 2017/3.

Froomkin, A. Michael – Colangelo, P. Zak: Self-Defense Against Robots and Drones. Connecticut Law Review 2015/1.

Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017.

Gless, Sabine – Silverman, Emily – Weigend, Thomas: If Robots Cause Harm, Who is to Blame? Self-driving Cars and Criminal Liability. New Criminal Law Review 2016/3.

Greene, Joshua D.: Solving the Trolley Problem. In: Sytsma, Justin – Buckwalter, Wesley (ed.): A Companion to Experimental Philosophy. John Wiley & Sons, Ltd. Chichester, 2016.

[25] Részletesen lásd Westbrook, Clint W.: The Google Made Me Do It: The Complexity of Criminal Liability in the Age of Autonomous Vehicles. Michigan State Law Review 2017/1. 97-147. o.

GURNEY, Jeffrey K.: Sue my Car not Me: Products Liability and Accidents Involving Autonomous Vehicles. Journal of Law, Technology & Policy 2013/3.

HAGE, Jeep: Theoretical foundations for the responsibility of autonomous agents. Artifical Intelligence and Law 2017/3.

HANNA, Katherine L.: Old Laws, New Tricks: Drunk Driving and Autonomous Vehicles. Jurimetrics 2015/3.

HODULA Máté: Az önvezető járművek és a büntetőjogi felelősség. Jogelméleti Szemle, 2018/3.

LIN, Patrick et al.: From Autonomous Cars to Artificial Intelligence, Oxford University Press. Oxford, 2017.

LOHMANN, Melinda Florina: Liability Issues Concerning Self-Driving Vehicles. The European Journal of Risk Regulation 2016/2.

SOMOGYI Zoltán: A bódult vagy ittas állapotban elkövetett bűncselekményekért való felelősség. Collega, 2005/2.

U.S. Department of Transportation's New Policy on Automated Vehicles Adopts SAE International's Levels of Automation for Defining Driving Automation in On-Road Motor Vehicles

WEIGEND, Thomas: Notstandsrecht für selbstfahrende Autos? Zeitschrift für Internationale Strafrechtsdogmatik 2017/10.

WESTBROOK, Clint W.: The Google Made Me Do It: The Complexity of Criminal Liability in the Age of Autonomous Vehicles. Michigan State Law Review 2017/1.

CSÁK ZSOLT

A DRÓNOK KAPCSÁN FELMERÜLŐ EGYES BÜNTETŐ ANYAGI ÉS ELJÁRÁSI JOGI KÉRDÉSEK[1]

1. Alapvetés

Repülő drónoknak alapvetően a pilóta nélküli repülő eszközöket[2] nevezzük, melyek közé tartozik a kézi vezérlésű játékhelikoptertől a komolyabb, quadrocoptereken át a milliós értékű, programozható eszközökig bármilyen drón.[3] A köztudomással ellentétben nem elsősorban az amerikai hadsereg által felderítésre vagy légicsapás mérésre használt pilóta nélküli repülőgépekre kell gondolnunk, hanem azon pilóta nélküli – okos repülőgépekre is – amelyeket katasztrófa sújtott területen használnak felderítésre, károk felmérésére, illetve kisebb szállítmányok (pl. gyógyszerek) célba juttatására, vagy akár csomagküldési célokra. Használják őket erdészeti és árvízvédelmi feladatokra, illetve egyre elterjedtebb a fotózásra, illetve videózásra történő igénybe vételük, amint azt számos sportesemény közvetítése kapcsán megtapasztalhattuk.

A tudósok ma már kísérleteket folytatnak kézi irányítás nélkül, önálló repülésre képes drónok kifejlesztésére is.[4] Ezek esetleges csoportos alkalmazása az egy eszköz által nehezen lefedhető nagyobb területen, vagy hosszú ideig tartó folyamatos megfigyelés esetén is igénybe vehető.

---

[1] A tanulmány a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) által a távirányított repülők (drónok) használatából eredő adatvédelmi és a magánélet sérthetetlenségét biztosító megfontolásokról Budapesten, 2015. február 5-6. napján rendezett nemzetközi konferencián elhangzott előadás szerkesztett, továbbfejlesztett és hatályosított változata.

[2] Az angolszász szakirodalomban gyakran használt mozaikszóval élve: UAV („unmanned aeriel vehicle").

[3] Átfogóan lásd PALIK Mátyás (szerk.): Pilóta nélküli repülés profiknak és amatőröknek. Második, javított kiadás. NKE, Budapest, 2013., DOUGHERTY, Michael J.: Drones: An Illustrated Guide to the Unnamed Aircraft that are Filling Our Skies. Amber Books Limited, Phoenix, 2015. és ELLIOT, Alex: Drónok kézikönyve. Cser Kiadó, Budapest, 2017.

[4] Ehhez lásd CHENG, Hong: Autonomous Intelligent Vehicles. Theory, Algorithms, and Implementation. Springer, London, 2011.

A nem katonai, azaz polgári használatban álló repülő drónok általában nem különböznek a távirányítású repülő- vagy helikopter modellektől. Tartalmaznak egy kisméretű fedélzeti számítógépet, és általában egy kamerát. Működtethetők Wi-Fin keresztül, rádiókapcsolaton, okos telefonról, tabletről, vagy kifejezetten erre készített irányító készülékről.

A civil felhasználók közé elsősorban a légi felvételeket használó sportközvetítések tartoznak, de igénybe veszik ezeket a régészek, térképészek, árvízvédelmi szakemberek és meteorológusok is. Igénybe vehetők továbbá mezőgazdasági megfigyelésekre is.

Utalni kell azonban arra is, hogy mind az Európai Unióban, mind Magyarországon a drónok egyre nagyobb számban jelennek meg, noha jelentős mértékben hiányzik a nemzeti és az uniós szabályozás.[5] Ugyanakkor katonai, bűnüldözési, kereskedelmi, tudományos és magáncélú felhasználásuk napról napra, egyre jobban terjed.

Felmerült ezért az igénye annak, hogy a hatóságok kezeljék azon aggályokat, amelyek a magánélet zavartalanságának biztosítása körül ezen jelenség kapcsán támadtak.[6] Indokolt javaslatokkal ellátni a jogalkotókat, az iparági és piaci szereplőket, valamint a magáncélú felhasználókat is a törvényes felhasználás érdekében.

Nem lehet vitás, hogy a repülő drónok használata kihatással lehet az alapvető emberi és szabadságjogokra.[7]

Magyarországról elmondható, hogy a repülő eszközökre és azok használatára a légügyi törvényben írtakat kell alkalmazni, ugyanakkor a drónok használatához a Nemzeti Média- és Hírközlési Hatóság által kiadható frekvencia-engedélyre is szükség van. Meg kell ugyanakkor felelni a légi távérzékelés engedélyezésének és a távérzékelési adatok használatának rendjéről szóló jogszabályoknak is. A bűnül-

[5] Az európai uniós szintű szabályozás – az EASA (Európai Repülésbiztonsági Ügynökség) ajánlásai alapján – 2019-re várható, illetve az eredetileg 2017 nyarára tervezett hazai rendeleti szabályozásra is várni kell még. Az Európai Unió jelenleg egységesnek nevezhető szabályozással még nem rendelkezik. Az egyetlen eldöntött kérdés, hogy az EU 216/2008/EK számú rendelete alapján, valamennyi Európában megtalálható 150 kg feletti drón az EASA hatáskörébe tartozik, amelyeket a hagyományos repülőeszközökhöz hasonlóan regisztrációkötelesek. Jelen helyzetben a 150 kg alatti eszközök szabályozása a tagállami szabályozás körébe tartozik. A Tanács 2006. február 27-i 394/2006/EK Rendelete alapján külön kategóriába, kettős felhasználású termékek közé tartoznak a 300 km feletti hatótávval illetve 500 kg hasznos tömeg feletti teherbírással rendelkező drónok, így birtoklásuk és exportjuk egyedi engedélyhez kötött.

[6] Takahashi, Timothy T.: Drones and Privacy. The Columbia Science&Technology Law Review. 2012/3. 72-114. o.

[7] Mérget, Frédériric: The Humanitarian Problem with Drones. Utah Law Review. 2013/5. 1283-1319. o. és Knoops, Geert-Jan Alexander: Drones at Trial: State and Individual (Criminal) Liabilties for Drone Attacks. International Criminal Law Review 2014/1. 42-81. o.

dözés körében nem lehet vitás az sem, hogy mind az Alkotmányvédelmi Hivatal, mind a Terrorelhárítási Központ és a Nemzetbiztonsági Szakszolgálat is érdekelt lehet a repülő drónok alkalmazásában.

Kiemelt jelentőséget kell tulajdonítani azon eseményeknek, amelyek során a repülő drónok balesetet okoznak. Magyarországon is előfordult már, hogy fesztiválon emberek közé zuhant drón.

Sajnálatos tény, hogy ugyan a Légügyi Hivatal számtalan engedélykérelmet vizsgál évente, de ugyanakkor ezek többszöröse esetében állapítható meg, hogy illegálisan röptetnek drónt.

Ezek a légi közlekedés biztonságára is kihatással lehetnek, hiszen a repülőgépek vagy helikopterek pilótái csak akkor veszik észre ezen eszközöket, amikor a baleset már nem hárítható el. Ennek kapcsán nem hagyható figyelmen kívül, hogy a mentő vagy rendőrségi helikopterek, valamint a katasztrófavédelem légi járművei szabadon használják a légtér részeit, azaz, nem a légi útvonalakon közelítik meg elsősorban céljukat.

Ilyen esetekben előfordulhat, hogy a repülő drónok képzetlen kezelője nem képes elhárítani a balesetet a szabályosan közlekedő légi jármű felbukkanása esetén. Szükséges ezért a szabályozás annak érdekében, hogy a légi irányításért felelős hatóság folyamatosan lássa, érzékelje a repülő drónt, és értesíteni, vagy utasítani tudja annak használóját a baleset lehetősége esetén.

A magyar jogi szabályozás tekintetében az is megállapítható, hogy csak eseti, vagy korlátozott légtér igénybe vételére vonatkozó engedéllyel és tevékenységi jóváhagyással lehet drónt röptetni, maximum 150 méteres magasságig, és 25 kg-nyi tömeghatárig. A Légügyi Hivatal biztosítja a kért koordináták által határolt terület légterét, ahol más légijármű nem jelenhet meg munkavégzés ideje alatt.

Ugyanakkor megállapítható – miként az Európa legtöbb országában is megfigyelt jelenség –, hogy a drón-használók legtöbbje nem rendelkezik légi jármű vezetésére vonatkozó hivatalos képesítéssel. Különösen igaz ez pl. a játékboltokban megvásárolt eszközök használói esetén. Ilyenkor igazolni kellene a hatóság felé, hogy a használó a pilóta nélküli légijármű használatára vonatkozó felelősségbiztosítással, kezelési és karbantartási útmutatóval rendelkezik.

Ez azonban Magyarországon nem számon kérhető, és számtalan olyan forgalmazó van, amely az értékesített eszköz használati oktatását elvégzi, de számos olyan is, amely erre nincs berendezkedve.

Mindezek a kérdések felvetik annak igényét, hogy a repülő drónok használatát a büntető anyagi jog és eljárásjog szempontjából is vizsgáljuk. Célom ezért annak bemutatása, hogy a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.), valamint a büntetőeljárásról szóló 2017. évi XC. törvény (a további-

akban: új Be.)[8] milyen mértékben alkalmas a repülő drónok által keltett problémák kezelésére.

Ulpianus szerint: „A jog szabályai a következők: tisztességesen élni, mást nem sérteni, mindenkinek megadni a magáét."

Ezen bölcsesség olyan korból származik, amikor a technikai fejlődés még kisebb problémák elé állította mind a jogalkotót, mind a jogalkalmazót. A „mást nem sérteni" elve azonban napjainkban újabb és újabb szabályozási igénnyel jelentkezik a jogalkotó számára.

Az emberi méltóság, az általános cselekvési szabadság, a magánszféra, valamint az élet- és a testi épség szabadságának Alaptörvény által védett érdekeit ma már a repülő drónok is képesek veszélyeztetni.

A játékoktól, a katonai célú felhasználásig, a közlekedés biztonságán át jogos igények merülnek fel a szabályozás iránt.

A büntetőbíró azonban elsősorban a következményeket vizsgálja, amelyek a repülő drónok használata kapcsán jelentkeznek. Ezek lehetnek negatív következmények, amennyiben bűncselekmény történik, illetve pozitív hatásuk is észlelhető, abban az esetben, ha a repülő drón büntetőeljárás során felhasználható bizonyítékot szolgáltat.

Ebből kiindulva, személyes véleményem, hogy jelenleg új jogi szabályozás az általunk vizsgált jogterületeken alapvetően nem szükséges. A napjainkban felmerülő problémákat mind a Btk., mind az új Be. megfelelő módon képes kezelni. Azaz, mind a balesetek, mind a szándékos bűncselekmények, illetve a bizonyítás kérdései a hatályos törvényünk alapján – túlnyomó részben – megoldhatóak.

Természetesen előfordulnak olyan esetek is, amikor a jelenlegi szabályozás nem alkalmazható a repülő drónok alkalmazása körében. Ebben a körben elsősorban talán a jogos védelem (Btk. 21-22. §) és a magánlaksértés (Btk. 221. §) kérdése vizsgálható.

Számunkra ezért a büntetőjogon kívüli jogalkotás igénye fogadható el, illetve a Btk. és az új Be. csupán kisebb mértékű módosítása.

Határozott véleményem, hogy a Btk. Különös Részébe új törvényi tényállás megállapítása nem szükséges. Ennek érdekében – a teljesség igénye nélkül – igyekszem bemutatni olyan bűncselekményeket, amelyek repülő drón jogellenes alkalmazása esetén felhasználhatók. Engedély nélküli, vagy esetlegesen regisztráció nélküli használat esetében legfeljebb szabálysértést tartok elképzelhetőnek; ebben az esetben helye lehet új szabálysértési tényállás alkotásának. Ebben a gondolatkörben különös tekintettel kell lenni a játékboltok rendkívül széles „választékára".

Ugyancsak hasonló – szabálysértés – lehet pl. az engedélytől (akár ferekvencia) eltérő használat is.

[8] Hatályba lépett 2018. július 1. napján.

2. A Btk. alkalmazásának kérdései drónok viszonylatában

2.1. A jogos védelem

A büntető anyagi jog területén az elsődleges probléma a jogos védelem kérdésének megítélésénél jelentkezik.[9]

A Btk. 22. § (1) bekezdése alapján nem büntetendő az a cselekmény, amely a saját, illetve más vagy mások személye, javai, vagy a közérdek ellen intézett, illetve ezeket közvetlenül fenyegető jogtalan támadás elhárításához szükséges.

Az nem lehet vitás, hogy a drón képes lehet támadni az Alaptörvényben foglalt olyan releváns jogokat, mint az élet, szabadság és a személyi biztonság.[10]

Ugyanakkor a vizsgált jogintézmény kapcsán számos probléma merül fel. A jogos védelem ugyanis alapvetően embertől származó támadás elhárítására szolgál. Mind a gyakorlat, mind a jogirodalom csupán az aktív emberi magatartást vizsgálta, és ennek kapcsán értelmezte a jogos védelem kérdését.[11]

Előfordulhat ugyanakkor természetesen, hogy a saját, vagy más személye vagy javai elleni támadást közvetett módon, műszaki eszköz által is megvalósítható.

A tipikus példa azonban a személy testi épsége elleni támadás. Kérdés, hogy ilyennek minősülhet-e a drón embereknek történő szándékos nekivezetése; amelyre eddig gyakorlati példa nem volt. A tárgyi javak ellen nehezen elképzelhető, hiszen ez inkább elsősorban a katonai célú felhasználást feltételezi, amelyben a büntetőjog ezen jogintézményének értelemszerűen nincs szerepe. Ráadásul ez a fajta „felhasználás" lényegében együtt jár a drón elvesztésével is.

A következő kérdés, hogy a védekező magatartásnak ki ellen kell irányulnia. A drón mint műszaki eszköz, vagy az azt irányító személy ellen.

Könnyebben értelmezhető a támadás intézett mivoltja abban az esetben, ha a drón működik, vagy közvetlen támadással fenyeget.

Ennek megítélése pl. egy ingatlan fölé reptetett drón esetén rendkívül nehéz. Aligha tekinthetjük intézett támadásnak azt, ha kertünk fölött azért röpköd egy drón, mert azzal valaki játszik, vagy akár rólunk akar jogsértéssel felvételeket készíteni.

---

[9] Az észak-amerikai szakirodalomban ezt a kérdéskört behatóan vizsgálja A. Michael Froomkin, A. Michael – Colangelo, P. Zak: Self-Defense against Robots and Drones. Connecticut Law Review. 2015/1. 36-56. o.

[10] A jogintézmény bemutatásához a recens szakirodalomból lásd Belovics Ervin: Büntetőjog I. Általános Rész. HVG-ORAC, Budapest, 2017. 240-259. o. és Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó, Budapest, 2017. 261-286. o.

[11] A 4/2013. BJE szerint ugyanakkor, amennyiben az aktív magatartással megvalósuló támadás jogellenes állapotot eredményez, annak fenntartása érdekében a támadó által tanúsított passzív magatartás is jogtalan támadásnak minősül.

További probléma a gyakorlat azon értelmezése, mely szerint a támadást nem kell kivárni, elegendő, ha az közvetlenül fenyeget. A kérdés, hogy vajon lelőhető-e a drón, amelyről az feltételezhető, hogy személyem ellen támadást intéz.

A fenti kérdésfeltevés nyilvánvalóan képtelennek tűnik, hiszen a jogos védelem a támadó személye ellen irányul, aki viszont esetünkben nem is biztos, hogy a látókörben van, és a megtámadott személy észlelni képes.

A fenyegető támadás megítélése pedig még nehezebb, a társadalomra veszélyességben való tévedés [Btk. 20. § (2) bek.], azaz a vélt jogos védelem esetén, amely sokkal gyakrabban lehet megállapítható ezekben az esetekben.[12]

A szükséges elhárítási módok meghatározása pedig szinte lehetetlen, mert nem tudjuk, hogy a drón ellen, vagy az irányító ellen vehetők-e igénybe. További probléma, hogyan vizsgálható a szükségesség egy géppel szemben, amely adott esetben rendkívül kisméretű is lehet. A játékboltokban ma már olyan készülékeket is lehet vásárolni, amelyek szándékos embernek történő nekivezetése esetén sem okoznak sérüléseket. Ugyanakkor előfordulnak olyan nagyobb méretű – pl. televíziós közvetítésre használt – repülő drónok, amelyek lezuhanása tényleges sérülések okozására alkalmas. További kérdés az irányító ellen alkalmazott esetleges erőszak esetén, hogy a megtámadott személy feltételezheti-e, hogy mit okozhatott volna a gép, illetve mit várhatunk el a megtámadottól, hogy az ő tudata mit fog át a kezelő esetleges magatartása, szándéka kapcsán.

Jogos védelem esetén a gyakorlat kimunkálta a túllépés kérdését is. Repülő drónnál azonban ez már problémát jelenthet mind az eszköz, mind az irányító esetében. Az ijedtség, és a menthető felindulás [Btk. 22. § (3) bek.] természetesen ebben az esetben is elképzelhető, de hasonló esetek előfordulása esetén még a gyakorlatra vár ezen kérdés megválaszolása. Különösen igaz lehet ez abban az esetben, hogyha a „támadás" pillanatában a megtámadott személy számára nem látható, nem elérhető a kezelő. Nyilvánvalóan el fog telni bizonyos idő, mire felfedezi a drón irányítóját, és vele szemben valamilyen büntetőjogilag értékelendő magatartást tanúsít. Gyakorlat hiányában legfeljebb vélelmezni lehet, hogy ez valószínűleg a túllépés körében lesz majd vizsgálható. A kérdéskör megítélése körében egyelőre az EBH 2007. 1584. számú határozatban foglalt iránymutatást alkalmazhatjuk, mely szerint a birtokvédelem körében alkalmazott önhatalom is megalapozhatja a jogos védelem megállapíthatóságát.[13]

[12] BH 1983.261.

[13] A kérdéskörhöz részletesen lásd Ujvári Ákos: A jogos védelem és a birtokvédelem viszonya az EBH 2007.1584. számú határozatban. Jogelméleti Szemle 2010/4. (http://jesz.ajk.elte.hu/ujvari44.html) és Ambrus István: Polgári jogi elemek a büntető anyagi jogban. Polgári Jog 2017/3. (online elérhető a Wolters Kluwer Jogtárban)

Természetes, hogy a kérdés megítélése „tényállás függő". A drónok ingatlan feletti zavaró reptetése megvalósíthatja a birtokvédelem körében alkalmazott önhatalom előfordulását. Nyilvánvaló, hogy a gyakorlat fogja ezt a kérdést majd értelmezni, miként azt is, hogy a támadó jellegű, vagy azzal közvetlenül fenyegető magatartás alapozhatja csak meg drón esetében is a jogos védelmet. A puszta zavarás és birtokháborítás nyilvánvalóan ebbe a kérdéskörbe nem vonható.

Összességében látható, hogy jogos védelem esetében a gyakorlat, és esetleg a jogi szabályozás kisebb mértékű változása adhat majd megoldást.

2.2. A magánlaksértés

A másik problémás kérdés a magánlaksértés értelmezése. A Btk. 221. § (1) bekezdése nem hagy kétséget afelől, hogy a bűncselekményt az követi el, aki más lakásába, egyéb helyiségébe vagy ezekhez tartozó bekerített helyre erőszakkal, fenyegetéssel vagy hivatalos eljárás színlelésével bemegy, illetve ott bent marad.

Látható, hogy drón esetében a cselekmény nem értelmezhető. A törvényi tényállás kétségen kívül a magánélet zavartalanságát védi, bűncselekmény vagy szabálysértés[14] is lehet az elkövetési magatartás következménye.[15] Jogi tárgya a lakás, egyéb helyiség, az ahhoz tartozó bekerített hely zavartalan használatához fűződő érdek, vagyis, alapvetően a magánlakás.[16]

Probléma lehet azonban az elkövetési tárgy körében a lakás, egyéb helyiség, bekerített hely, amely általában kert, telek lehet, és elsősorban itt fordulhat elő a repülő drón használata. Ugyanakkor az ingatlan feletti légteret a gyakorlatnak eddig soha nem kellett értelmeznie, soha nem kellett állást foglalni abban a kérdésben, hogy ezen a területen magánlaksértés bekövetkezhet-e, vagy sem.

A második probléma, hogy csak akkor tényállásszerű a cselekmény, ha a bent lévő jogosulttal szemben valósul meg. Továbbá, a bemenetel az egész testtel való bejutást jelenti. Ebből következően pedig nem a drónnak, hanem az elkövetőnek kell bejutni. Ezért is fogalmaz úgy a törvényi tényállás, hogy aki bemegy, vagy bent marad.

Mindezek alapján – egyelőre – az állapítható meg, hogy a repülő drón mint eszköz a magánlaksértés „elkövetője" nem lehet. Ezt legfeljebb a kezelő valósítja meg,

[14] A szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény (Szabs. tv.) 166. §

[15] BH 2014.357., BH 2016.106.

[16] Belovics Ervin: Magánlaksértés. In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál: Büntetőjog II. Különös Rész. A 2012. évi C. törvény alapján. Második, hatályosított kiadás. HVG-ORAC, Budapest, 2013. 263. o.

így azonban értelmetlennek tűnik a bűncselekmény elemzése, hiszen ez utóbbi esetben az eddigi gyakorlat szerint kell a cselekményt megítélni.

Végül, az utolsó probléma, hogy az elkövetés módja is tényállási elem: erőszakkal vagy fenyegetéssel, illetve hivatalos eljárás színlelésével kell ezt megvalósítani. Ezek nélkül ugyan a szabálysértés megvalósul, de az elkövetési magatartás, és az elkövetés tárgya ugyanaz. Erőszak, fenyegetés eszközzel is megvalósítható, azonban a törvény nem hagy kétséget afelől, hogy ezt nem eszköznek, hanem a személynek, élő embernek kell megvalósítania. A fentiek ellenére sem tartom indokoltnak a repülő drónok miatt a magánlaksértés törvényi tényállásának módosítását, ugyanakkor az elkövetési magatartás jellegére figyelemmel a szabálysértési jogszabály változás már elképzelhető lehet.

2.3. Zaklatás

Repülő drón jogsértő alkalmazása esetén teljes mértékben elképzelhetőnek tartom a zaklatás törvényi tényállásának alkalmazását.[17] A Btk. 222. § (1) bekezdése alapján, aki abból a célból, hogy mást megfélemlítsen, vagy más magánéletébe, illetve mindennapi életvitelébe önkényesen beavatkozzon, őt rendszeresen, vagy tartósan háborgatja, vagy félelemkeltés céljából azt a látszatot kelti, hogy más életét, testi épségét vagy egészségét sértő vagy közvetlenül fenyegető esemény következik be.

A bűncselekmény jogi tárgya az emberi méltóság és a magánszférához való jog.[18] Elkövetési magatartása elsősorban a háborgatás. Ez alkalmatlankodás, mások megzavarása útján valósul meg. Azaz, bármely nyugtalanságot keltő tevékenység alkalmas lehet a zaklatás megállapítására. A cselekménynek ugyanakkor alkalmasnak kell lennie a mindennapi életvitel megnehezítésére. Ebbe viszont a repülő drónok alkalmazása is értelmezhető.

Nem hagyható figyelmen kívül azonban, hogy nem általános magatartásról, hanem célzatos cselekményről van szó. Azaz, a zaklatás megvalósulásához az szükséges, más rendszeres vagy tartós háborgatása a megfélemlítés, vagy a magánéletébe, illetve mindennapi életébe önkényes beavatkozás céljából történjen.[19] A cselekményt tehát egyenes szándékkal követhető el. Ilyen lehet olyan játékcélú felhasználás, amely szándékosan figyelmen kívül hagyja az ingatlanok határait, és alkalmas mások nyugalmának megzavarására, pl. a drón okozta hanghatással, vagy olyan fajta röptetéssel, amely magában hordozza a sérülés alkalmazásának lehetőségét.

---

[17] Az újabb jogirodalomban lásd Ambrus István – Ujvári Ákos: A zaklatás bűncselekményének gyermekévei. Magyar Jog 2016/7-8. 424-435. o., Bérces Viktor: A zaklatás törvényi tényállásába ütköző cselekmények minősítése és bizonyítási kérdései. Magyar Jog 2017/7-8. 454-462. o.

[18] Belovics Ervin: Zaklatás. In: Belovics – Molnár – Sinku: i. m. 269. o.

[19] BH 2011.268.

További feltétel a zaklatás első fordulata vonatkozásában, hogy a háborgatás rendszeres, vagy tartós legyen. Azaz, általában hosszabb időn keresztül, folyamatosan, visszatérően nyugtalanítja az elkövető a sértettet.

A gyakorlat azonban részben a technikai eszközök alkalmazását már kimunkálta, hiszen az elkövetési magatartás bármi lehet, és a jogértelmezés ide sorolja a technikai eszközöket is, mint pl. sms-ek, e-mailek használatát. De az elkövetési magatartás körében értelmezhető a követés, a lakóhely szemmel tartása is, amely repülő drón útján is megvalósul.

A Btk. 222. § (3) bekezdése alapján súlyosabban büntetendő, aki a zaklatást házastársa, volt házastársa, élettársa, vagy volt élettársa sérelmére valósítja meg (egyebek mellett).

Az már nem lehet vitás, hogy ilyen jellegű magatartás a repülő drón felhasználásával is elkövethető, hiszen a sértett követése, a levegőből való nyugtalanítása – az egyéb törvényi feltételek megvalósulása esetén – egyértelműen tényállásszerű lehet.

2.4. Becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése

A repülő drón használata megvalósíthatja továbbá a Btk. 226/A. §-ában foglalt becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése bűncselekményét. Ezen tényállást az követi el, aki abból a célból, hogy más vagy mások becsületét csorbítsa, hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt készít.

A bűncselekmény célzata a becsület csorbítása hamis, hamisított vagy valótlan tartalmú felvétel készítése útján. Ezen bűncselekménynek a repülő drón eszköze lehet. Abban az esetben, ha pl. légi felvételt készítenek valamely személyről, annak tudta, beleegyezése nélkül, és az így elkészített felvételt pl. montázs útján meghamisítják, és olyan módon használják fel vagy hozzák nyilvánosságra, amely alkalmas a becsület csorbítására.

2.5. Közlekedési bűncselekmények

A repülő drónok által megvalósított jogellenes magatartások körében jelentős helyet foglalhatnak el a közlekedési bűncselekmények.[20] Elsősorban a közlekedés biztonsága elleni bűncselekményt kell vizsgálni.

A Btk. 232. § (1) bekezdése alapján ezt a bűncselekményt az követi el, aki közlekedési útvonal, jármű, üzemi berendezés vagy ezek tartozéka megrongálásával vagy megsemmisítésével, akadály létesítésével, közlekedési jelzés eltávolításával vagy megváltoztatásával, megtévesztő jelzéssel, közlekedő jármű vezetője ellen erőszak

[20] Viski László: Közlekedési büntetőjog. Közgazdasági és Jogi Könyvkiadó, Budapest, 1974. 308-309. o.

vagy fenyegetés alkalmazásával vagy más hasonló módon más vagy mások életét vagy testi épségét veszélyezteti.

Ezen bűncselekmény tehát a repülő drónok igénybe vétele esetén szinte minden esetben alkalmazható, még akkor is, ha egyébként semmilyen külső szabályozás a repülő drónokra vonatkozóan nincs.

Ennek elkövetője ugyanis – extraneus – kívülálló. Csak olyan lehet, aki nem áll meghatározott közlekedési szabályok hatálya alatt. Amennyiben igen, úgy más bűncselekményt, közúti veszélyeztetés (Btk. 234. §) vagy vasúti, légi vagy vízi közlekedés veszélyeztetése (Btk. 233. §) jöhet szóba.

A bűncselekmény valamely közlekedési ágazat biztonságához fűződő érdek védelmét szolgálja, amely lehet mind vasúti, légi, vízi vagy közúti. A törvényhozó mind a szándékos, mind a gondatlan magatartást bünteti, melynek eredménye a veszélyhelyzet. Nem kell ténylegesen baleset, ha azonban ez mégis bekövetkezik, a cselekmény súlyosabban minősül, de a tényállásszerűséghez elég az absztrakt veszélyhelyzet is.

Elsődleges relevanciája az elkövetési magatartásnak van, amely megvalósulhat akadály létesítésében, ami bármi lehet, amennyiben annak következtében nem lehetséges a közlekedés biztonságos lebonyolítása.

Relevánsabb azonban a jármű vezetője elleni erőszak vagy fenyegetés. Ez a bűncselekmény passzív alanya és haladásban lévő jármű esetén valósul meg.

A gyakorlat egyértelmű abban, hogy a cselekmény dologgal szemben is megvalósulhat, de amennyiben áttevődik a vezetőre, úgy a magatartás tényállásszerű. Ilyen pl. a vasúti mozdonyok kővel való megdobálása.

Releváns elkövetési tárgy a közlekedési útvonal, vagy a közlekedési jármű. Az útvonal fogalma kellően tág, hiszen abban légtér és a légi folyosó is beletartozhat. A gyakorlatban ugyanakkor értelmezhető olyan légtér is, amely nem tartozik szorosan a légi folyosó kategóriájába. A bevezetőben már utaltunk a rendőrségi, vagy mentőhelikopterekre, amelyek lényegében szabad útvonalon közlekednek, és bárhol megjelenhetnek olyan területen, ahol pl. repülő drónok röptetése történik.

A cselekmény tehát bármely területen megvalósulhat, amely közlekedésre igénybe vehető.

Összefoglalva, a repülő drón olyan jellegű alkalmazása, amely repülőgép, helikopter, vízi- vagy közúti jármű vezetőjét akadályozza, mert pl. szándékosan, vagy gondatlanul a vezető elé reptetik, és ezzel baleset veszélyét idéznek elő, tényállásszerű, és a bűncselekmény megállapítására lehet alkalmas.

Minden olyan esetben, amikor a repülő drónokra vonatkozóan már van szabályozás, a vasúti, légi vagy vízi közlekedés veszélyeztetése kerülhet szóba.

A Btk. 233. § (1) bekezdés alapján a fenti bűncselekményt az követi el, aki a vasúti, a légi vagy a vízi közlekedés szabályainak megszegésével más vagy mások életét vagy testi épségét veszélyezteti.

Ma már köztudomású tény, hogy a katonai célú repülő drónok lényegében nagyméretűek és üzemeltetésük szabályosan, repülőtérről történik. Ezen két körülmény figyelembe vételével megállapítható, hogy rájuk a légi közlekedés szabályai vonatkoznak. Ezek megszegése ezért a fenti bűncselekmény megállapítására alkalmas, és nyilvánvaló, hogy külön büntetőjogi szabályozást nem igényel.

2.6. Foglalkozás körében elkövetett veszélyeztetés

Alkalmazható bűncselekménynek tartom a foglalkozás körében elkövetett veszélyeztetést is. A Btk. 165. § (1) bekezdése szerint ezt az valósítja meg, aki foglalkozási szabály megszegésével más vagy mások életét, testi épségét vagy egészségét gondatlanságból közvetlen veszélynek teszi ki, vagy a közvetlen veszélyt szándékosan idézi elő.

Repülő drón esetében is akkor valósulhat meg ezen cselekmény, ha van valamilyen szabályozás. Ez mind írott vagy szakmai, akár íratlan szabály is lehet. Amennyiben ezek megszegése okozati összefüggésben veszélyhelyzetet és/vagy balesetet, sérülést okoz, a bűncselekmény minden további nélkül megállapítható. Itt vetődik fel azonban először az esetleges szabályozási igény, de ez is büntetőjogon kívül, oly módon azonban, melynek értelmezése a bűncselekményi tényállás megállapítását segítheti elő.

A foglalkozás körében elkövetett veszélyeztetés ugyanis foglalkozási szabály megszegésével követhető el. A cselekmény ugyanakkor limitált veszélyeztetési szándékot foglal magába, vagyis a szándék csak a veszélyhelyzetre terjedhet ki. Repülő drón esetében a vonatkozó szabályok szándékos megszegésével képzelhető ez el (alapeseti vegyes bűnösség).

A gyakorlatból példát is tudunk felhozni az értelmezés megkönnyítésére. Eszerint, foglalkozás körében elkövetett veszélyeztetés vétségét és nem közlekedés biztonsága elleni bűncselekményt valósít meg, aki a közlekedés biztonságát nem aktív magatartásával veszélyezteti, hanem a foglalkozása szabályainak megszegésével gondatlanságból idézi elő a veszélyhelyzetet.[21] Ilyen lehet pl. a repülő drón nem megfelelő karbantartása, akkumulátorának elégtelen feltöltése és az ennek következtében történő lezuhanás okozta veszélyhelyzet.

Elképzelhetőnek tartom, hogy pl. munkavégzésre használt drónok esetében már egyértelműen beszélhetünk „íratlan szakmai szabályokról". Játékok esetében azon-

[21] BH 2011.156.

ban indokolt lehet valamilyen szabályozás, mégpedig olyan, amely a forgalmazó számára kötelezővé teszi, hogy ezt megismertesse a vásárlóval, adott esetben még ezt regisztráció is elősegítheti, amely nyomon követhetővé és számon kérhetővé teszi a szabálytól eltérő felhasználást és esetlegesen akár büntetőjogi, akár közigazgatási jellegű felelősségre vonást.

A drónra vonatkozóan ugyanis kezelési, karbantartási szabályok minden további nélkül felállíthatók. Példaként elképzelhető, hogy sportesemény közvetítése kapcsán olyan kamerát magában foglaló repülő drónt alkalmaznak, amelynek előzetes műszaki ellenőrzését, szervizelését elmulasztották, nem ellenőrizték az akkumulátorok feltöltöttségi szintjét, és ennek következtében az eszköz a játékosok vagy a nézők közé zuhan, és személyi sérülést, adott esetben halált is okoz. Nem lesz kétséges annak megállapítása, hogy a kezelőtől elvárható lett volna, hogy csak megfelelő műszaki állapotban lévő drónt röptessen emberek fölé. Különösen igaz ez azon munkavégzésre használt eszközök esetében, amelyek a játékcélú felhasználásnál lényegesen nagyobbak, súlyosabbak, és további eszközöket is magukban foglalnak, azaz egyértelműen különösebb vizsgálat nélkül is alkalmasak sérülés vagy halál okozására.

2.7. Rongálás

Álláspontom szerint a repülő drónnal vagyon elleni bűncselekmények is elkövethetők. Ezek közül elsősorban a rongálás jöhet szóba. A Btk. 371. § (1) bekezdése szerint aki idegen vagyontárgy megsemmisítésével vagy megrongálásával kárt okoz, rongálást követ el.

Szükséges utalni arra, hogy a bűncselekménynek gondatlan alakzata (ma már) nincs, azaz, csak abban az esetben állapítható meg, ha valaki a repülő eszközt szándékosan vezeti neki más vagyontárgyának és okozza annak megsemmisülését vagy megrongálását.

A polgári célú repülő drónok felhasználása elsősorban megfigyelés, fényképezés, filmezés céljából történik. Alkalmas lehet ezért az üzleti titok megsértése bűncselekményének megállapítására is.

2.8. Adatszerzéssel elkövethető bűncselekmények

A Btk. 418. §-a alapján, aki jogtalan előnyszerzés végett, vagy másnak vagyoni hátrányt okozva üzleti titkot jogosulatlanul megszerez, felhasznál, más személy részére hozzáférhető tesz vagy nyilvánosságra hoz, ezen bűncselekményt valósítja meg.

A kamerával ellátott repülő drón esetében nem lehet vitás, hogy üzleti titok jogosulatlan megszerzésének az eszköze lehet.

Az üzleti titok megsértése bűncselekményének elkövetési magatartása a megszerzés. Lényegében nyitott tényállásról beszélünk, amely bármilyen módon meg-

valósítható.[22] Ilyen lehet pl. egy autógyártó üzem kísérleti telepén lefolytatott új modellek tesztelésével kapcsolatos események lefilmezése.

Amennyiben a titkokat csak dokumentum formájában fogadjuk el, nyilvánvalóan a bűncselekmény abban az esetben állapítható meg, ha ezek lefotózására vagy lefilmezésére képes a repülő drón, ez azonban – véleményem szerint – sokkal inkább a kémfilmek világába tartozik, sem mint a mindennapokban megvalósuló tényállásszerű magatartások körébe.

Kevésbé lehet vitás, hogy a repülő drónnal elkövethető a tiltott adatszerzés bűncselekménye.[23] A Btk. 422. § (1) bekezdés a), b) és d) pontjában foglalt magatartás jöhet figyelembe. Eszerint, aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából más lakását, egyéb helyiségét vagy az azokhoz tartozó bekerített helyet titokban átkutatja, más lakásába, egyéb helyiségébe vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy rögzíti, illetve elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti, a tiltott adatszerzés bűncselekményét valósítja meg.

A bűncselekmény célja a magántitok, gazdasági vagy üzleti titok megismerése. A releváns elkövetési magatartás a megfigyelés, vagy technikai eszköz alkalmazásával történő rögzítés. Azaz, bármilyen, nem titkos szolgálatok által alkalmazott módszer figyelembe jöhet. Feltétele, hogy mindez titokban, a passzív alany által fel nem ismerhető módon történhet.

Problémát lényegében az elkövetés helye okozhat, hiszen kizárólag magánlakás, annak egyéb helyisége vagy azokhoz tartozó bekerített helyen valósulhat meg, vagyis nem csak a lakáson belül. Optikai, elektronikai eszközökkel, kamerával, fényképezőgéppel vagy egyéb lehallgató eszközök felszerelésével a repülő drón alkalmas lehet ezen magatartás tanúsítására.

Persze kérdés, hogy üzleti vagy gazdasági titkot nem biztos, hogy magánlakásban, vagy egy udvari fürdőmedence mellett figyelhet meg az ingatlan fölé berepülő drón.

Álláspontom szerint itt már felmerül a jogi szabályozás igénye, hiszen a repülő drónok alkalmazására figyelemmel az elkövetés helyét ki kellene terjeszteni gazdasági, ipari létesítményekre és azokhoz tartozó ingatlanokra, ahol nagyobb eséllyel valósulhat meg gazdasági illetőleg üzleti titkok megismerése, megfigyelése.

Az informatika fejlődésének következtében – értelemszerűen – elterjedtek az ahhoz kapcsolódó illegális magatartások. Azaz, személyek képesek arra, hogy infor-

[22] Ehhez lásd Gellér – Ambrus: i.m. 209-215. o.

[23] Molnár Gábor Miklós: Tiltott adatszerzés. In: Belovics – Molnár – Sinku: i.m. 879-884. o.

mációs rendszerbe jogellenesen behatoljanak. Ezen a magatartás kapcsán elsősorban az ún. „hacker"-ekre kell gondolni.[24] Ugyanakkor a Btk. teljes körű szabályozásának köszönhetően még az ún. légi hackerekkel szemben is találunk törvényi tényállást.

Ilyen a Btk. 423. §-ában megfogalmazott információs rendszer vagy adat megsértése bűncselekménye, melyet az követi el, aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép. Mindez elkövethető olyan technikai eszközzel, amelyet repülő drónra szerelnek, és azt olyan rendszer vagy eszköz közelébe juttatják, amelyből az információt igyekeznek megszerezni. Kétségtelen, hogy egyfajta XXI. századi bűncselekményről beszélhetünk, azonban a büntető törvény kész ezen probléma kezelésére.

A fentiekre figyelemmel az már nem is lehet kétséges, hogy a repülő drón eszköze lehet a kémkedés bűncselekménye megállapításának is. A Btk. 261. §-a lényegében nyitott törvényi tényállást tartalmaz, hiszen elkövetési magatartása a hírszerző tevékenység folytatása, amely lényegében bármi lehet, nyilvánvaló ezért, hogy pl. katonai objektumok illegális megfigyelése repülő drón útján is megvalósulhat.

Végül, a büntető anyagi jog alkalmazása szempontjából a jogosulatlan titkos információgyűjtésre vagy adatszerzésre kell utalni. Ennek elkövetési magatartása a Btk. 307. §-a alapján az engedélyhez kötött titkos információgyűjtést, illetve adatszerzés engedély nélküli végzése, vagy az engedély kereteinek túllépése. Nem vitás, hogy ennek a repülő drón eszköze lehet. Természetesen csak abban az esetben valósul meg bűncselekmény, ha külső engedély keretében értelmezhető cselekményről van szó.

A repülő drón abban az esetben értendő ide, ha vonatkoztatható rá az új Be. 232. § (3) bekezdésében foglalt feltétel, azaz, hely titkos megfigyelése során a leplezett eszközök alkalmazására feljogosított szerv bírói engedéllyel – a nyilvános vagy a közönség részére nyitva álló hely kivételével – a lakásban, egyéb helyiségben, bekerített helyen, illetve – a közösségi közlekedési eszköz kivételével – járművön történteket titokban technikai eszközzel megfigyelheti és rögzítheti. Ennek engedély nélküli, vagy engedélyt meghaladó alkalmazása esetén nyilvánvaló a bűncselekmény megállapíthatósága. A cselekményt csak hivatalos személy követheti el, melyből következően nem lehet kizárt, hogy titkos információgyűjtést vagy adatszerzést folytató állami hatóságok repülő drónt is igénybe vehetnek. Ezt jelenleg jogszabály számukra nem tiltja. Jogellenes felhasználás esetén azonban a bűncselekmény megállapításának lehet helye.

[24] Mezei Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. Magyar Jogászegyleti Értekezések 9-10. Budapest, 2018. 158-167. o.

2. Az új Be. rendelkezései és a drónok egyes összefüggései

A repülő drónok alkalmazása nemcsak bűncselekmény megállapítására lehet alkalmas, hanem felveti a büntetőeljárás körében a bizonyításra vonatkozó szabályok vizsgálatát. Nem lehet kétséges, hogy repülő drón szolgáltathat olyan bizonyítékot, amely az új Be. vagy a büntető anyagi jog alkalmazása során a bizonyítás szempontjából releváns lehet. Elöljáróban leszögezhető határozott álláspontom, hogy az új Be. módosítása sem szükséges a repülő drónokra tekintettel.

Jellegénél fogva az új Be. 204. §-a szerinti tárgyi bizonyítási eszközként értékelhető, lényegében mind a drón, mind az általa szolgáltatott bizonyíték.

Ennek megítélésénél jelentősége van az új Be. 204. § (2) bekezdésében foglalt kiterjesztő értelmezésnek, mely szerint irat minden olyan tárgyi bizonyítási eszköz, amely műszaki, vegyi vagy más eljárással adatokat rögzít. Az (1) bekezdés szerint pedig az irat tárgyi bizonyítási eszköz. Nem vitás, hogy ilyennek minősül tehát a drón is.

Ilyen jellegű műszaki eszközt számtalan esetben használnak fel a büntetőeljárás során a bizonyítás céljából. Ilyen lehet pl. az ipari-kamera felvétele, amely bankrablást rögzít, helikopterről készített felvétel, a tv társaságok büntetőeljárásában felhasznált felvételei, vagy rendőrségi felvételek, pl. tömegzavargások esetén.

A repülő drón ezért a bizonyítás körében hasznos lehet mind információ megszerzésére, mind pedig pl. követés felhasználására. Az alkalmazásnak azonban értelemszerűen törvényi korlátai lehetnek. Ilyen elsősorban a bizonyítás törvényessége. Ezen belül is a lefoglalás és a bizonyítási eszközök kezelésének törvényessége.

Az új Be. 166. § (1) bekezdése ugyanis nem hagy kétséget afelől, hogy a bizonyítási eszközök felderítése, összegyűjtése, biztosítása és felhasználása során e törvény rendelkezései szerint kell eljárni. A büntetőeljárásról szóló 1998. évi XIX. törvény (a továbbiakban: régi Be.) 77. § (2) bekezdés pedig előírta, hogy a bizonyítási cselekmények végzésekor az emberi méltóságot, az érintettek személyiségi jogait, és a kegyeleti jogot tiszteletben kell tartani és biztosítani kell, hogy a magánéletre vonatkozó adatok szükségtelenül ne kerüljenek nyilvánosságra. Ezek a jogok az új Be.-ben már mint alapelvek jelennek meg a törvény 2. §-ában.[25]

[25] „Az alapvető jogok védelme

2. § (1) A büntetőeljárásban tiszteletben kell tartani mindenkinek az emberi méltóságát.

(2) A büntetőeljárásban mindenki számára biztosítani kell a szabadsághoz és személyi biztonsághoz fűződő jogot.

(3) A büntetőeljárásban alapvető jogot korlátozni csak az e törvény szerinti eljárásban, az e törvényben meghatározott okból, módon és mértékben lehet, feltéve, hogy az elérni kívánt cél kisebb korlátozással járó más eljárási cselekmény vagy intézkedés útján nem biztosítható."

Ezen tiltó és garanciális szabályok azonban nem minden esetben jelentik a felhasználás kizártságát. Hiszen az új Be. 167. § (1) bekezdése a bizonyítékok értékelése körében azok szabadságának elvéből indul ki, mivel a büntetőeljárásban szabadon felhasználható a törvényben meghatározott minden bizonyítási eszköz. Csupán a bűncselekmény útján, tiltott módon vagy a résztvevők eljárási jogainak lényeges korlátozása útján szerzett bizonyíték felhasználása tilos. A gyakorlatra vár e körben értelmezni a repülő drónt, illetőleg az általa szolgáltatott bizonyítékot. Azonban a tisztesség elve és a tisztességes eljárás követelménye a repülő drón által szolgáltatott bizonyíték esetén is figyelembe veendő.

Ebben a körben sajátos helyzetet teremt a mérgezett fa gyümölcsének értelmezése.[26] Kontinentális jogrendszerünk általában ezen angolszász felfogást nem osztja. Azaz, nem minősül más tiltott módon vagy a résztvevők eljárási jogainak lényeges korlátozásával szerzett bizonyítéknak, ha a vizsgálandó és felhasználandó tény normasértéssel beszerzett bizonyítási eszközből ered. Ennek különös jelentősége van pl. a repülő drónok által szolgáltatott információk esetén abban az esetben, ha maga a felhasználás illegálisnak minősül.

Képzeljük el azt az esetet, ha valaki üdülő övezetben az ingatlanok felett azért reptet videokamerával vagy fényképezőgéppel felszerelt eszközt, mert illegálisan szeretne felvételeket készíteni ruhátlanul napozó hölgyekről abból a célból, hogy azt akár valamely közösségi oldalon megjelenítse. Ugyanakkor azonban valamely személy sérelmére elkövetett bűncselekményt, pl. rablást rögzít, amely egy magánlakás kertjében történik. Abban az esetben, ha az így készült felvételt a büntetőeljárás szabályai szerint a bűnüldöző hatóságok lefoglalják, nem tartom kizártnak a felvétel felhasználását a bizonyítási eljárás során. Feltétel azonban, hogy a személyiségi jogok megsértése büntető és polgári következményekkel járhat, azaz a magánéletre vonatkozó adatok szükségtelenül nem kerülhetnek nyilvánosságra, vagyis az új Be. 2. §-a és 167. § (5) bekezdésében foglaltak szem előtt tartásával kerülhet sor az így készült felvétel felhasználására. Akkor viszont nem minősül jogellenesnek a személyiségi jog sérelme, ha bizonyíték megszerzése érdekében szükséges a felhasználás, azzal a kitétellel, hogy illetéktelen személy tudomására természetesen nem hozható.

Mindezek azonban feltételezések, egyelőre a büntetőeljárásban még nem találkoztunk repülő drón által szolgáltatott bizonyítékkal, vagy esetlegesen már láttunk ilyen felvételt, csak nem tudtuk, hogy az ilyen eszközből származik. Különös jelentősége van a titkos adatszerzés és a titkos információgyűjtés körében a repülő drónnak.

[26] A legújabb hazai szakirodalomban lásd Elek Balázs: A „mérgezett fa gyümölcsének elve" a hazai és a strasbourgi joggyakorlat türkében. Magyar Jog 2018/2. 94-104. o.

Az előzőekben már utaltam rá, hogy jogszabályok nem tiltják, hogy ezen bizonyítási eljárás során repülő drónt alkalmazzanak. A kérdés elsősorban ott merül fel, hogy külső engedélyhez kötött eszköznek, vagy ezen kívülállónak kell-e a repülő drónt tekinteni. Mind a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 54. § (1) bekezdése, mind a Rendőrségről szóló 1994. évi XXXIV. törvény 66. § (1) bekezdése azonos módon szabályozza azt a kérdést, mely szerint nem kell bírói engedély például épület külső megfigyelésére, objektum, terep, útvonal, jármű, esemény, személy megfigyelésére, vagy ezen megfigyelés rögzítésére.[27]

Az új Be. 232. § (3) bekezdés alapján azonban – mint arra fentebb már történt utalás – külső engedélyhez kötött valamely hely titkos megfigyelése, vagy – a nyilvános vagy a közönség részére nyitva álló hely kivételével – a magánlakásban, illetve – a közösségi közlekedési eszköz kivételével – járművön történtek titokban technikai eszközzel megfigyelése és rögzítése. Vagyis, a titkos kutatás és megfigyelés már engedélyhez kötött.

A kérdés, hogy a repülő drón lehet-e olyan technikai eszköz, amely a fenti jogszabályok körébe tartozik. Az új Be. ezeket nem sorolja fel, ezért értelemszerűen a repülő drón is ebbe a körbe tartozhat. Azt pedig már az alkalmazás jellege dönti el, hogy engedélyhez kötött, vagy külső engedélyhez nem kötött módon kerül sor a felhasználásra.

Lényegében nem látok különbséget a titkos adatszerzés és a titkos információszerzésre vonatkozó szabályok között a drónok megítélése kérdésében. Az alapvető következtetés ezért az, hogy a repülő drón alkalmazása ma egyik formában sem kizárt.

A bizonyítási eljárás során azonban érdekes lehet a régi Be. 206. § (1) bekezdésében foglaltak összevetése a repülő drón által szolgáltatott információval. Eszerint ugyanis, ha az ügyész a titkos adatszerzés eredményét a büntetőeljárásban bizonyítékként kívánja felhasználni, a titkos adatszerzés engedélyezése iránti indítványt, a bíróság határozatát, és a titkos adatszerzés végrehajtásáról készített jelentést csatolja a nyomozás irataihoz.[28] Azaz, elsősorban okirati bizonyíték formájában jelennek meg az eredmények. Az természetesen nem lehet vitás, hogy tárgyi bizonyítási eszközként kell felhasználni az elkészített felvételeket. A technikai eszköz jellege ezért

[27] Ehhez átfogóan lásd Boda József: A felderítés, hírszerzés, titkos információgyűjtés elvei és gyakorlata. Belügyi Szemle 2015/9. 5-29. o.

[28] Ezen idézett szabályt az új Be. explicite ugyan már nem jeleníti meg, a tárgyi bizonyítási eszköz fentebb már idézett, mikénti szabályozásából azonban implicite következik, hogy továbbra is ebben a formában juthat el az így beszerzett bizonyítási eszköz a bírósághoz.

legfeljebb a végeredményből derül ki, pl. a légi felvétel leírása, vagy megtekintése útján. Ebben az esetben sem biztos, hogy mindig nyilvánvaló a felhasználó számára az, hogy ezt repülő drón készítette.

Összességében tehát, a büntetőeljárási jogban különösebb problémákat nem lehet felállítani, illetve ezek előfordulása esetén azok a törvény szerint megoldhatók.

3. Összegzés

Az Alkotmánybíróság a 2/2007. számú határozatában fejtette ki, hogy a bűnüldözés kockázata az államot terheli. Ez pedig csak anyagi és eljárási jogszabályok által meghatározott rendben folyhat. Azaz, a magánélet tiszteletben tartása mind Magyarország Alaptörvényének VI. cikke, mind a Polgári és Politikai Jogok Nemzetközi Egyezségokmánya[29] szempontjából releváns. Ugyanakkor azonban ezen kérdés megítélésénél – álláspontom szerint – a repülő drón nem különbözik a manapság általánosan használt eszközöktől.

A titkos eszközök alkalmazása a közrend vagy közbiztonság és a nemzetbiztonság védelme céljából indokolt az Alkotmánybíróság szerint. Nyilvánvaló, hogy kivételesen, ultima rátióként lehet figyelembe venni akkor, ha nyílt eljárásban alkalmazható eszközök nem elegendőek, a felderítés pedig kilátástalan.

Összességében tehát – álláspontom szerint – a büntető anyagi jog és büntetőeljárási jog szempontjából vizsgálva a távirányított repülők alkalmazását, szükséges rámutatni arra, hogy jelenleg is rendelkezésre állnak olyan jogszabályok, amelyek az alkalmazásuk, felhasználásuk, illetőleg a tiltott alkalmazás következményeinek megállapítása szempontjából relevánsak és figyelembe vehetőek. Felmerül ugyanakkor számos kérdés, amely a drónok jellege folytán további jogi szabályozást igényel. Felhasználásuk ugyanis olyan problémákat valószínűsít, amelyek nem feltétlenül oldhatók meg a jelenlegi szabályozás keretei között.

Jogi szabályozás azonban véleményem szerint elsősorban a közlekedés biztonsága, a foglalkozási szabályok, az engedélyezési eljárás, valamint a nyilvántartási és regisztráció körében, valamint esetlegesen a szabálysértés keretei között képzelhető el.

[29] Magyarországon kihirdette az Egyesült Nemzetek Közgyűlése XXI. ülésszakán, 1966. december 16-án elfogadott Polgári és Politikai Jogok Nemzetközi Egyezségokmánya kihirdetéséről szóló 1976. évi 8. törvényerejű rendelet, melynek 17. Cikk 1. pontja szerint "Senkit sem lehet alávetni a magánéletével, családjával, lakásával vagy levelezésével kapcsolatban önkényes vagy törvénytelen beavatkozásnak, sem pedig a becsülete és jó hírneve elleni jogtalan támadásnak."

Említést érdemel végül, hogy jelenleg is számos olyan megfigyelésre alkalmas eszköz használata történik (pl. bűnüldöző hatóság, illetve a sajtó képviselői által készített videofelvételek), amelyek hasonló problémákat vetnek fel, alkalmazásuk, illetve felhasználásuk törvényességével kapcsolatban azonban a büntető anyagi jog és büntetőeljárási jog szempontjából jelentős problémák nem merültek fel.

Felhasznált irodalom

Ambrus István – Ujvári Ákos: A zaklatás bűncselekményének gyermekévei. Magyar Jog 2016/7-8.

Ambrus István: Polgári jogi elemek a büntető anyagi jogban. Polgári Jog 2017/3.

Belovics Ervin: Büntetőjog I. Általános Rész. HVG-ORAC, Budapest, 2017.

Belovics Ervin: Magánlaksértés. In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál: Büntetőjog II. Különös Rész. A 2012. évi C. törvény alapján. Második, hatályosított kiadás. HVG-ORAC, Budapest, 2013.

Belovics Ervin: Zaklatás. In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál: Büntetőjog II. Különös Rész. A 2012. évi C. törvény alapján. Második, hatályosított kiadás. HVG-ORAC, Budapest, 2013.

Bérces Viktor: A zaklatás törvényi tényállásába ütköző cselekmények minősítése és bizonyítási kérdései. Magyar Jog 2017/7-8.

Boda József: A felderítés, hírszerzés, titkos információgyűjtés elvei *és* gyakorlata. Belügyi Szemle 2015/9.

Cheng, Hong: Autonomous Intelligent Vehicles. Theory, Algorithms, and Implementation. Springer, London, 2011.

Dougherty, Michael J.: Drones: An Illustrated Guide to the Unnamed Aircraft that are Filling Our Skies. Amber Books Limited, Phoenix, 2015.

Elek Balázs: A "mérgezett fa gyümölcsének elve" a hazai *és* a strasbourgi joggyakorlat türkében. Magyar Jog 2018/2.

elliot, Alex: Drónok kézikönyve. Cser Kiadó, Budapest, 2017.

Froomkin, A. Michael – Colangelo, P. Zak: Self-Defense against Robots and Drones. Connecticut Law Review. 2015/1.

Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó, Budapest, 2017.

Knoops, Geert-Jan Alexander: Drones at Trial: State and Individual (Criminal) Liabilties for Drone Attacks. International Criminal Law Review 2014/1.

MÉRGET, Frédériric: The Humanitarian Problem with Drones. Utah Law Review. 2013/5.

MEZEI Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. Magyar Jogászegyleti Értekezések 9-10. Budapest, 2018.

MOLNÁR Gábor Miklós: Tiltott adatszerzés. In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál: Büntetőjog II. Különös Rész. A 2012. évi C. törvény alapján. Második, hatályosított kiadás. HVG-ORAC, Budapest, 2013.

PALIK Mátyás (szerk.): Pilóta nélküli repülés profiknak és amatőröknek. Második, javított kiadás. NKE, Budapest, 2013.

TAKAHASHI, Timothy T.: Drones and Privacy. The Columbia Science&Technology Law Review. 2012/3.

UJVÁRI Ákos: A jogos védelem és a birtokvédelem viszonya az EBH 2007. 1584. számú határozatban. Jogelméleti Szemle 2010/4.

VISKI László: Közlekedési büntetőjog. Közgazdasági és Jogi Könyvkiadó, Budapest, 1974.

DORNFELD LÁSZLÓ

KIBERTERRORIZMUS – A JÖVŐ TERRORIZMUSA?

1. Bevezetés

A terrorizmus, amely a '80-as évek vége óta egyre kevésbé volt jelentős Európában, napjainkban újra egyre nagyobb fenyegetést jelent a kontinensre. A közelmúltban végrehajtott párizsi és brüsszeli támadások megmutatták a lakosság sebezhetőségét az ilyen támadásokkal szemben. A hagyományos terrorizmus ismételt megjelenését látva nő az azzal kapcsolatos félelem is, hogy a terroristák az informatikai rendszerek felhasználásával is képesek lehetnek csapást mérni. Ez igen jelentős biztonsági kockázatot jelentene, hiszen ezen új technológiai vívmányok lassan minden európai lakos mindennapi életének részévé váltak. Ráadásul az internetes környezet jóval ideálisabb körülményeket teremt a terrorcselekmények elkövetésére.

Habár a kiberterrorizmus kifejezés már 1979-ben megjelent egy svéd számítógépes bűnözésről szóló jelentésben,[1] széles körben csak a 9/11-i terrortámadásokat követően terjedt el a büntetőjogi szakirodalomban.[2] Érdemes megjegyezni, hogy politikai célú támadásokat már ezt megelőzően is indítottak az interneten keresztül, így például az 1999-es koszovói konfliktus során. A Jugoszláviát ért bombázásokat követően túlterheléses, ún. DDoS-támadások (Distributed Denial of Service)[3] indultak a NATO weboldalaival szemben,[4] és jugoszláv honlapok működését is megpróbálták ellehetetleníteni vagy tartalmukat módosítani. A NATO szándékosan nem pusztította el az ország internetelérést biztosító fizikai infrastruktúráját, abban bízva, hogy az interneten keresztül szerzett információk a jugoszláv kormány ellen fordíthatják a lakosságot.[5]

---

[1] Oleksiewicz, Izabela: Dilemmas and Challenges for EU Anti-Cyberterrorism Policy: The Example of the United Kingdom. Teka Kom. Politol. Stos. Międzynar. 2016/3. 136. o.

[2] Parti Katalin: Kerekasztal-beszélgetés az online terrorizmusról. Ügyészek Lapja, 2010/2. 43. o.

[3] Lásd bővebben Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1. 66-83. o

[4] Sipos Zoltán: A kibertér biztonságával kapcsolatos alapvető kérdések áttekintése. Honvédségi Szemle, 2016/1. 28. o. (Denning (2001): i.m. 252. o.)

[5] Denning, D. E. : Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing

Fontos kérdés ugyanakkor, hogy ezek az akciók tekinthetők-e kiberterrorizmusnak. A jogi szakirodalom közel sem egységes abban a kérdésben, hogy hol húzódik a határ az internetes polgári engedetlenség és a terrorizmus között. Tovább nehezíti az elhatárolást, hogy napjainkban a terrorszervezetek egyre gyakrabban élnek a kibertér adta lehetőségekkel saját üzeneteik terjesztésére, a követők toborzására és pénzügyi támogatás szerzésére. Ez a folyamat szintén az 1990-es években kezdődött meg, amikor az egyes csoportok elkezdték létrehozni saját honlapjaikat.[6] Ezek száma alig párról 2007-re már 4300-ra nőtt,[7] és napjainkra a terrorszervezetek aktívan használják az internetet. Jó példa erre, ahogyan az Iszlám Állam a közösségi média aktív és profi felhasználásával gyorsan hírhedté vált, és viszonylag széles online támogatói kört tudott kiépíteni.

E fejezetben áttekintem a jogirodalomban jelen lévő álláspontokat, valamint elhatárolási kísérleteket. A fogalom meghatározás és elhatárolás mellett a kiberterrorizmus jellemzőit is bemutatom, valamint azt, hogy az egyes államok milyen módszerekkel igyekeznek az ilyen támadásokat megelőzni, illetve a mögötte állókat felderíteni. Ezek mellett arra is választ keresek, hogy napjainkban mennyire jelent aktuális biztonsági fenyegetést az internetes terrorizmus, és várható-e ennek változása a jövőben.

2. A kiberterrorizmus meghatározása

A kiberterrorizmus szó nyelvtani értelemben vizsgálva a kibertérben elkövetett terrortámadásokat jelöli. Ennek megértéséhez meg kell vizsgálnunk a két fogalom jelentését. A kiber a görög kübernétészből (κυβερνήτης) ered, amely kormányost jelent. Az angolban ismertté William Gibson tette, aki 1982-ben használta először a kibertér fogalmát a fizikai világtól elkülönülő digitális térre.[8] A terrorizmus a latin terrere (megrémít) szóból ered, amelyet a francia -isme toldalékkal ellátva megkapjuk a terrorisme-et. Ez már a „rémületet okozni" jelentéssel bír.[9]

Foreign Policy. In: J. Arguilla, D. Ronfeldt (ed.) = Networks and Netwars: The Future of Terror, Crime, and Militancy. 2001. 239-241. o.

[6] Denning: i. m. 252. o.

[7] Hummel, Michael L.: Internet Terrorism. Homeland Security Review 2008/2. 117. o.

[8] Wall, David S.: Cybercrime: The Transformation of Crime in the Information Age. Polity, 2007. 10–11. o. Megjegyzendő ugyanakkor, hogy sok helyen tévesen Gibsont jelölik meg, mint a fogalom megalkotóját. http://www.kunstkritikk.dk/kommentar/the-reinvention-of-cyberspace/ [2018.06.23.]

[9] Matusitz, Jonathan: Terrorism & Communication. A Critical Introduction. Thousand Oaks, SAGE Publications, 2013. 1. o.

Ezen fogalmak egyikének sincs egységes meghatározása a jogirodalomban. A kibertér leginkább a mai internet keretei között értelmezhető, de tágabb annál. Fogalmát Frédérick Douzet úgy próbálta megragadni, hogy az „emberek, adatok és számítógépek hálózata… információs tér, területhez nem kötött információcsere, amelyet nehéz megérteni. Materiális infrastruktúrából áll, amelyet fizikai területre építenek, ideértve a világűrben megtalálható műholdakat is."[10]

A terrorizmus szabályozásával 14 ENSZ egyezmény és 4 kiegészítő jegyzőkönyv is foglalkozik, ezek mindegyike megkerüli azonban az egységes fogalom kérdését, ehelyett egy-egy elkövetési módozat fogalmát megadva csupán. Ennek következtében napjainkra mintegy ötven különböző cselekményt rendelnek üldözni a releváns nemzetközi egyezmények, ami nagyfokú bizonytalanságot okoz.[11] Hosszú ideje sikertelenül próbálják elfogadni a Nemzetközi Terrorizmusról szóló Átfogó Egyezmény Tervezetet, amely szerint a terrorcselekmények olyan „másik állammal szemben végrehajtott, személy vagy dolog elleni erőszakos cselekmények, amelyek természetükből adódóan a közéleti szereplőkben, személyek csoportjában, a közvéleményben vagy a lakosságban rémületet, félelmet vagy bizonytalanságot keltenek".[12]

Ebből a meghatározásból máris kitűnik a legnagyobb probléma a kiberterrorizmus koncepciójával kapcsolatban: személy vagy dolog elleni erőszakos cselekmények szerepelnek benne. Eltérő megközelítést alkalmaz az Európai Unió 2017/541 irányelve[13] és az ezt megelőző 2002/475/IB tanácsi kerethatározat fogalmát a 2012. évi C. törvénybe (a továbbiakban Btk.) építő hazánk, ahol a tényállás előbb meghatározza a célzatot, majd az eszközcselekményeket. Ezek jelentős része is csak a fizikai világban megvalósítható cselekmény, azonban itt már számos olyat találhatunk, amely a kibertérben is megvalósítható. Így például a 3. cikk g) pontja szerinti „veszélyes anyag kiengedése, vagy tűzvész, árvíz vagy robbanás előidézése, amely emberi életet veszélyeztet". 2000-ben Ausztráliában egy hacker 800 ezer liter szennyvizet engedett a környező vizekbe, súlyos károkat okozva az élővilágnak.[14] A cikk h)

[10] Pintér István: A virtuális tér geopolitikája. In: Pintér István (szerk.) A virtuális tér geopolitikája. Geopolitikai Tanács, 2016. 312. o.

[11] Dornfeld László – Sántha Ferenc: A terrorizmus és a terrorcselekmény, mint nemzetközi bűncselekmény aktuális kérdései. Jog Állam Politika 2017/3. 73–75. o.

[12] Dornfeld – Sántha: i. m. 79–80. o.

[13] Az Európai Parlament és a Tanács 2017/541 irányelve a terrorizmus elleni küzdelemről. HL 2017 L 88, 31.3.2017. Elfogadták 2017. március 15-én, átültetés határideje 2018. szeptember 8.

[14] Environmental Risks: Cyber Security and Critical Industries. 5. o. Nevezett támadás ugyan más okból (politikai célzat hiánya) nem tekinthető terrorcselekménynek, de rámutat arra, hogy a terroristák is végrehajthatnak hasonló támadásokat.

pontjában szereplő „a víz- vagy áramellátásnak, illetve más létfontosságú természeti erőforrás ellátásának olyan megzavarása vagy megszakítása, ami emberi életet veszélyeztet" szintén végrehajtható a kibertérben. Az irányelv i) pontja és a Btk. a 314. § (4) bekezdés i) pontja egyaránt az eszközcselekmények közé sorolja a 2013/40/EU irányelvben szabályozott „rendszert érintő jogellenes beavatkozás" (a Btk. terminológiája szerint „információs rendszer vagy adat megsértése") bűncselekményét is.[15]

A kiberterrorizmus angolszász területen egyik népszerű meghatározása szerint „kiber rendszerek elleni erőszak, zavarás vagy működésébe történő beavatkozás vagy ezzel való fenyegetés, mikor valószínűsíthető, hogy ennek eredménye halál vagy sérülés, vagyontárgy súlyos károsodás vagy a társadalmi rend megzavarása."[16] Látható, hogy a fogalom alapvetően a terrorizmus megjelenési formáit és a kibertérben történő elkövetést vonja össze, és bizonyos elemeinél kiütközik az angolszász jogrendszer dogmatikai kötetlensége, például az erőszak szerepeltetésénél. Más fogalmak, így például Denningé szintén tartalmazzák az „erőszakos támadás" fogalmát.[17] Ugyanakkor, mint az a fentiekből is látható, a kontinentális jogrendszerekben a terrorcselekmény már létező tényállásának részeként szabályozzák a jelenséget, és így új fogalmat sem alkotnak rá.

3. Elhatárolása más kiberfenyegetésektől

A kibertérben jelen lévő fenyegetések között már régóta próbálnak a kutatók és az azok elhárításában részt vevő szervezetek különbséget tenni. Ez a kérdés nem csak elméleti jellegű, hiszen két hasonló kibertámadás esetén is előfordulhat, hogy más állami szerv fellépése szükséges. Egy bűncselekmény esetén ugyanis elegendő lehet a nyomozó hatóság fellépése, de ha a cél kémkedés vagy kiberháborús támadás végrehajtása volt, akkor a titkosszolgálat és a hadsereg válaszlépése szükséges. A szakirodalom alapvetően eltérő számú típusát határozza meg a kiberfenyegetéseknek,[18] én ezek közül a következőket gondolom relevánsnak a téma szempontjából: hacktivizmus, kiberbűnözés, kiberterrorizmus és kiberhadviselés. A fogalmaknagyon hasonlóak egymáshoz, hiszen mind valamilyen tevékenység kibertérben történő megvalósítását jelöli, így szükséges ezeket elhatárolni egymástól.

[15] Lukácsi Tamás: A terrorizmus elleni küzdelemről szóló (EU) 2017/541 európai parlamenti és tanácsi irányelv. Európai Jog 2017/6. 23. o.

[16] Gillespie, Alisdair A.: Cybercrime – Key Issues and Debates. Routledge, 2016. 107. o.

[17] Mezey Nándor Lajos: Kiberterrorizmus: valós veszély? Belügyi Szemle, 2011/2. 23. o.

[18] Maras, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017. 378. o.

3.1. Hacktivizmus

A hacktivizmus kifejezés a hackelés és aktivizmus szavak összerántásából született meg. Jellegét nézve tekinthetjük a hackermozgalom politikai kifejeződésének, politikai célzatú hackelésnek vagy politikai célok hackereszközökkel való elérésnek.[19] Az internet közvéleményt formáló ereje – mint arra már a bevezetőben is utaltam – már hosszabb ideje, legalább a koszovói konfliktus óta ismert. A háború során mindegyik harcban álló fél igyekezett az internetet a saját üzenetének terjesztésére hasznosítani, de e tevékenységek többsége egyszerű internetes aktivizmus volt.[20] Az egyik első komolyabb politikai célú támadásra azonban már egy évtizeddel korábban, 1989-ben sor került, amikor a NASA és az Egyesült Államok Energiaügyi Hivatalának számítógépeit törték fel, és a bejelentkező képernyőt nukleáris energia elleni üzenetekre módosították.[21] Szemben az aktivizmussal, amely az internet nyújtotta legális lehetőségeket – például online petíciók írása, figyelemfelkeltő honlapok és blogok létrehozása – használja fel valamely vélemény szélesebb körű terjesztésére, a hacktivizmus már illegális vagy jogilag aggályos eszközök igénybevételét jelenti. Ez tipikusan az ellenkező véleményen lévő weboldalak vagy kormányzati portálok feltörését, elérésének megakadályozását jelenti, jellemzően minimális károkozással.[22] Példaként hozható az az eset, amikor 2012-ben a magukat az Anonymous hackerideológia követőiként azonosító elkövetők meghackelték az Alkotmánybíróság honlapját és megváltoztatták rajta az Alaptörvény szövegét.[23]

A hacktivizmus a kiberterrorizmushoz hasonlóan szintén a politikai célok elérését szolgálja, ám mégis szükséges külön kezelni a két jelenséget. Különösen azért, mert – mint arra Mezey Nándor is rámutat – vannak, akik tagadják az utóbbi létezését.[24] Denning szerint az utóbbit elkövetők céljaikat valamilyen súlyos veszteség, például halálozások vagy jelentős gazdasági kár előidézésével kívánják megvalósítani. Ezzel szemben a hacktivizmust a polgári elégedetlenség kibertérben történő megjelenéseként értelmezi.[25] Illig szintén hasonlóképp vélekedik a hacktivizmus szerepéről. Szerinte a hacktivisták legfőbb célja az internetes szólás- és információszabadság biztosítása, és módszerükben az különbözteti meg őket a kiberterroristáktól, hogy

[19] Simon Béla: Hacktivism and Its Status in Hungary. Magyar Rendészet 2016/2. 161. o.
[20] Denning: i. m. 246–250. o.
[21] Illig, A. T.: Computer Age Protesting: Why Hacktivism is a Viable Option for Modem Social Activists. Penn State Law Review, ?/2015. 1035–1036. o.
[22] Denning: i. m. 240–242. o.
[23] http://index.hu/tech/2012/03/04/az_anonymous_atirta_az_alaptorvenyt/ [2018. 06. 23.]
[24] Mezey: i. m. 23. o.
[25] Denning: i. m. 263. o.

elkötelezettek az erőszakmentes aktivizmus mellett.[26] WALL szerint a fő különbség a két besorolás között abban áll, hogy a kiberterrorizmus valamilyen kritikus infrastruktúrát vesz célba.[27] A kritikus infrastruktúra fogalmát a 2008/114/EK irányelvet átültető 2012. évi CLXVI. törvény 1. § tartalmazza: ez alapján ide tartozik minden olyan rendszerelem és létesítmény, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna. Egy példán keresztül szemléltetve: míg a magyarországi Anonymous korábban említett oldalfeltörése elhanyagolható anyagi kárt okozott, addig az Észtország online infrastruktúráját 2007-ben három hétig támadó orosz hackerek szinte teljesen megbénították az állam működését.[28]

3.2. Kiberbűnözés

Fontos kérdésként merül fel, hogy a kiberterrorizmus a kiberbűnözés részeként értelmezhető-e vagy pedig elkülönül attól. Egyes szerzők annak pártján állnak, hogy a jelenség a kiberbűnözés egyik megjelenési formája.[29] A kettő eszköztára ugyanis jelentős átfedést mutat, így például kártékony programok, elosztott szolgáltatásmegtagadással járó, avagy DDoS-támadás, információs rendszerbe történő jogosulatlan belépés mindkettőnél megfigyelhető.[30] Ugyanígy megegyeznek a támadások módszerei, amelyek arra irányulnak, hogy a rendszerek gyengepontjait használva adjanak hozzáférést a támadónak a rendszerhez. A legtöbb államban a két bűncselekményi körrel foglalkozó szervek is azonosak vagy legalábbis igen jelentős átfedést mutatnak.

A fő különbség az elkövetés mögötti motivációban lelhető fel. Míg a bűnözők elsősorban vagyoni vagy más előny eléréséért, esetleg szórakozásból követnek el bűncselekményeket a kibertérben, addig a kiberterrorizmus mögött valamilyen politikai, vallási indíttatású cél húzódik meg. További különbség még, hogy a terroristák sokkal szélesebb körben határozzák meg célpontjaikat, mint a bűnözők. A célok terén a fő különbség, hogy a terroristák a megkülönböztetés nélküli fizikai károkozást kívánják elérni, míg a bűnözők esetén ez nem kifejezetten cél.[31]

---

[26] ILLIG: i. m. 1036–1037. o.

[27] WALL: i. m. 9. o.

[28] BUONO, Laviero: Gearing Up the Fight Against Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). New Journal of European Criminal Law, 2012/3. 336. o.

[29] CASSIM, F.: Addressing The Spectre of Cyber Terrorism: A Comparative Perspective. Potchefstroom Electronic Law Journal, 2012. 381. o.

[30] Az egyes eszközök részletesebb leírásáért lásd: PATAKI Márta – KELEMEN Roland: Kiberterrorizmus. A terrorizmus új arca. Magyar Rendészet 2014/5. 106–109. o.

[31] BRENNER, W. Susan: Cybercrime, Cyberterrorism and Cyberwarfare. Revue internationale de droit pénal, 2006/3. 453–471. o.

Véleményem szerint ugyanakkor ez a különbségtétel legfeljebb elméleti szinten tehető meg, hiszen a gyakorlatban szinte lehetetlen teljesen egyértelműen eldönteni, hogy egy támadás mögött ki áll. Az eszközök és módszerek nagymértékű hasonlósága, a támadás mögötti cél homályossága folytán az éles elkülönítés esetén komoly hatásköri viták állhatnának elő, pontosan akkor, amikor gyors reakció szükséges a kiberbiztonság helyreállítása érdekében. Ebből kifolyólag én nem látom előnyét a kiberbűnözés és a kiberterrorizmus közötti éles határvonal meghúzásának, amely a jövőben is valószínűleg inkább akadémiai, semmint gyakorlati jellegű vizsgálati kérdés marad.

3.3. Kiberhadviselés

A kiberhadviselés az államok által indított kibertámadásokra alkotott fogalom, amelynek alapját képezi az, hogy a technológiai fejlődést az államok egyre gyakrabban a politikai és katonai erőfölény biztosítása érdekében használják fel.[32] Hadtudományi szempontból a NATO az információs műveletek részeként kezeli, amelyek célja az információs fölény elérése. Jellegét tekintve lehet támadó, amely az ellenség hálózatait célozza, valamint védekező, amely a saját rendszerek megóvására irányul. Lényeges az is, hogy kiberhadviselésről nemzetközi jogi értelemben akkor beszélhetünk, ha ismert a támadó állam kiléte.[33]

A fő különbség éppen ezért könnyedén megállapítható a kiberterrorizmus és a kiberhadviselés között: előbbinek nem állami szereplők, utóbbinak államok a végrehajtói. Ugyanakkor az állami érintettség kérdése az, amelyet igen nehéz bizonyítani, az államok ugyanis nem vállalják fel nyíltan a békeidőben végrehajtott kibertámadásaikat. Jó példa erre az, hogy a Snowden-botrány révénkiderült, az Egyesült Államok 2011-ben 231 alkalommal indított titokban támadást Oroszország, Kína, Irán és Észak-Korea ellen.[34] De ugyanígy nem bizonyítható az, hogy az Egyesült Államok és Izrael hajtotta végre az iráni atomlétesítmények elleni támadást a Stuxnet kártevővel,[35] annak ellenére, hogy a jelek egyértelműen rájuk mutatnak.[36]

---

[32] Szathmáry Zoltán: Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban. PhD értekezés. Budapest, 2012. 43. o.

[33] Berki Gábor: Kiberháborúk, kiberkonfliktusok. In: Pintér István (szerk.) A virtuális tér geopolitikája. Geopolitikai Tanács, 2016. 260–264. o.

[34] Eichensehr, Kristen E.: The Cyber-Law of Nations. Georgetown Law Journal, 2015/2. 319. o.

[35] Lásd részletesen: Nagy Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula – Hautzinger Zoltán: Pécsi Határőr Tudományos Közlemények XIII. 2012. 225-228. o.

[36] Lásd ehhez Holt, Thomas J. – Bossler, Adam M. – Seigfried-Spellar, Kathryn C.: Cybercrime and digital forensics: An introduction. Routledge, 2018. 411-415. o.

Szemben a kiberbűncselekménytől való elhatárolástól, itt gyakorlati jelentősége is lenne a különbségtételnek, hiszen teljesen más következményekkel járnak, és más szerveknek kell érintetté válnia. Kiberhadviselés esetén a diplomáciai-katonai válaszok foganatosításának kell megtörténnie, így például az Egyesült Államok kibertérre vonatkozó nemzetközi stratégiája leszögezi, hogy kibertérből érkező állami támadásra bármely eszközzel – legyen az diplomáciai, információs, katonai vagy gazdasági – válaszolhatnak.

4. Terroristák és az internet

A továbbiakban szükséges még egy elhatárolást megtennünk, méghozzá a kiberterrorizmus és a terroristák egyéb internetes tevékenysége között. Mint arra már a bevezetőben is utaltam, a terroristák és terrorszervezetek napjainkra már előszeretettel veszik igénybe az internet nyújtotta lehetőségeket, hiszen olcsón tudnak nagy közönséghez eljutni üzeneteik. Alapvetően ötféle célt különböztethetünk meg: propaganda, pénzgyűjtés, információterjesztés, biztonságos kommunikáció és hírszerzés.[37] Ezek a szervezet rendes működéséhez kapcsolódó tevékenységek, amelyeknél az új technológia igénybevétele könnyebbé vagy biztonságosabbá teszik addigi tevékenységeiket.

A propaganda a terrorszervezet online történő kommunikációját takarja, aminek célja a befolyásolás, és jelentheti céljaik, akcióik bemutatását és a toborzást is. Például csecsen terroristák weboldalukon közzétették egy lelőtt orosz gép képét, mivel Moszkva azt megelőzően tagadta ezt.[38] Érezhető a jelentős előrelépés, hiszen alig pár évtizede még csak otthon másolt kazettákon terjedhetett csak egy-egy szervezet ideológiája. A kommunikáció az internet igénybevételével nemcsak felgyorsult, de többirányúvá is vált, a magánkézben lévő nagy közösségi médiák pedig csak lassan reagáltak a terrorszervezetek megjelenésére. Az Iszlám Állam elsősorban a Twitter lehetőségeit használta ki, például a hashtagek használatával (#), amiknek a lényege, hogy az ezzel ellátott tartalmak együtt megtalálhatók és könnyen kereshetők, és így az aktuálisan felkapott témák közé a szervezet terrortámadásainak, lefejezéseinek képeit vegyítették. Ez annyira sikeresnek bizonyult, hogy 2014-ben a szervezet saját Twitter applikációt készített, amellyel ki tudták játszani a Twitter algoritmusait, és az azt telepítő felhasználók nevében üzeneteket küldeni.[39]

[37] Gillespie: i. m. 110. o.

[38] Warren, M. J.: Terrorism and the Internet. In: Janczewski, Lech J. – Colarik, Andrew M. (ed.): Cyber Warfare and Cyber Terrorism. Information Science Reference, 2008. 43. o.

[39] Besenyő János: Az Iszlám Állam. Terrorizmus 2.0. Kossuth Kiadó, Budapest, 2016. 157–161. o.

A pénzgyűjtés a terrorszervezetek működéséhez elengedhetetlen tevékenység, és már régóta bűncselekménynek számít a terrorizmus finanszírozása. Az internet számos lehetőséget kínál arra, hogy ezek a tevékenységek rejtve maradjanak a bűnüldöző hatóságok elől. Így például az Azzam Publications nevű oldal dzsihád témájú kiadványok árusításából juttatott összeget az Al-Kaida számára.[40] A terroristák számára más, a kiberpénzmosásban is használt eszközök is rendelkezésre állnak. Ilyenek például az online banki átutalások, a közvetítőkön, mint a PayPal keresztüli átutalások, a mobil fizetések és a különböző digitális pénzek, mint például a Bitcoin.[41] Ezeknél különösen nehéz ellenőrizni a tranzakciók végső címzettjét, és a több szereplőn keresztülfutó átutalások összege könnyedén számos kisebb összegre bontható, amelyek nem keltenek feltűnést.[42] A szervezetek adománygyűjtő számláira mutató elérhetőségeket pedig a közösségi médiában lehet könnyedén terjeszteni. Az online kaszinók szintén használhatók a terrorizmus finanszírozására.[43] Egy másik megoldás lehet, ha különböző kiberbűncselekmények elkövetéséből szereznek pénzt a szervezet működéséhez,[44] például zsarolóvírusok révén.[45]

Az információterjesztés abban különbözik a propagandától, hogy nem az embereket igyekszik megszólítani, hanem a terrorszervezet tagjai és szimpatizánsai számára közöl fontos tudnivalókat. Így például katonai mozgásokról, hogy elkerülhessék őket vagy a bombakészítés lépéseiről.[46] A már említett Azzam nevű weboldalon számos útmutató elérhető volt a dzsihád folytatásának módjaival kapcsolatosan.[47] A 87 halálos áldozattal járó 2016-os nizzai támadás elkövetője, Lahouaiej-Bouhlel is ilyen internetes forrásokból vette az ötletet az elkövetés módjához, a kamionnal történő tömegbe hajtáshoz.

A biztonságos kommunikáció azt az igényt szolgálja ki, hogy a terrorszervezetek tagjai a hatóságok számára láthatatlanul maradva tudják egymással a kapcsolatot fenn-

[40] Warren, M. J.: i. m. 43–44. o.
[41] Nagy Zoltán – Mezei Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog. 2018/70. 27-28. o.
[42] Tropina, Tatiana: Fighting money laundering in the age of online banking, virtual currencies and internet gambling. ERA Forum, 2014/1. 73–77. o.
[43] Nagy Zoltán András – Mezei Kitti: The organised criminal phenomenon on the Internet. Journal of Eastern-European Criminal Law. 2016/2. 143. o.
[44] Hummel: i. m. 120–121. o.
[45] Lásd Nagy Zoltán András – Mezei Kitti: A zsarolóvírus és a botnet vírus, mint napjaink két legveszélyesebb számítógépes vírusa. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Pécsi Határőr Közlemények XIX. Pécs, 2017.
[46] Gillespie: i. m. 111. o.
[47] Bozonelos, Dino – Stocking, Galen: The Effects of Counter-Terrorism on Cyberspace: A Case Study of Azzam.com. Journal of the Institute Of Justice & International Studies, 2003/3. 94. o.

tartani.[48] A CIA terrorelhárításért felelős vezetője szerint az internetes kommunikáció alapvetővé vált az Al-Kaida tagjai között, mivel ez nagyobb anonimitást biztosít nekik. Ebben igen fontos szerepe van a titkosításnak, amelyet az ezredforduló óta használnak egyre inkább.[49] Nagy segítséget nyújtanak számukra a kiberbűnözők által is előszeretettel használt „privát szférát erősítő technológiák".[50] Ilyenek például a virtuális magánhálózatok (VPN), amelyek segítségével a felhasználó könnyedén kaphat a világ bármely más országába mutató IP címet, illetve az Amerikai Egyesült Államok által katonai célokra kifejlesztett TOR (The Onion Router), amely igen nehezen feltörhető titkosítási módszerrel védi a kommunikáció tartalmát. A titkosításnak nemcsak a kommunikációban, hanem az adatok titkos tárolásában is szerepe lehet, így például a World Trade Center elleni 1993-as bombamerénylet kitervelője is ezzel a módszerrel élt.[51]

5. A kiberterrorizmus jellemzői

A kibertér sajátosságai jelentősen megkönnyítik a kiberbűnözők dolgát, és ilyenformán a potenciális kiberterroristákét is. Így például az internet globális jellege, amely nem teszi szükségessé, hogy személyesen is jelen legyenek az elkövetésnél. Hasonlóan fontos szempont az anonimitás is, hiszen lehetővé teszi, hogy maguk az elkövetők nehezen beazonosíthatók legyenek. Ráadásul az itteni működés sokkal olcsóbb, mint a tradicionális terror eszközei, és a lebukás esélye is jóval kisebb a támadást megelőzően. A támadáshoz nagyszámú célpont közül választhatnak, és ezek potenciálisan nagyobb számú ember életét képesek befolyásolni, mint egy hagyományos terrorcselekmény. Ebből eredő további előny az is, hogy jóval nehezebb védekezni a kibertámadásokkal szemben.[52] Ugyanakkor akadnak ellenérvek is az eszköz használata kapcsán, így például az, hogy megfelelő informatikai szaktudásra van szükség hozzá. Vagy a terroristák maguk szerzik meg ezt évek alatt vagy pedig már képzett hackerek segítségét veszik igénybe, de erősen kérdéses, hogy ők egyáltalán dolgoznának-e egy terrorszervezetnek.[53]

[48] MEZEY: i. m. 23. o.
[49] HUMMEL: i. m. 118. o.
[50] KISS Attila: A privátszférát erősítő technológiák. Infokommunikáció és jog 2013/56. 113–119. o.
[51] CASSIM: i. m. 385. o.
[52] MEZEY: i. m. 36–37. o.; OLEKSIEWICZ: i.m. 138–139. o.; valamint GYARAKI Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012. 235-236. o.
[53] GILLESPIE: i. m. 109. o.

A témával foglalkozó szakirodalom három fő fejlődési irányát különbözteti meg az informatikai terrorizmusnak: a tömeges pusztítást (weapon of mass destruction), a tömeges zavarkeltést (weapon of mass distraction) és a társadalmi rend szétzilálását (weapon of mass disruption).

A tömeges pusztítás a kritikus infrastruktúrát célzó támadásokat jelenti, amelyeknek célja a súlyos károkozás, például egy erőmű felrobbantása a rendszereinek a túlterhelésével. Ez Brenner megfogalmazásában csak elvi, és nem gyakorlati lehetőség, ami abból a téves feltételezésből ered, hogy a számítógépek képesek a 9/11-i terrortámadáshoz hasonló károkat okozni. Maguk a számítógépek ebben az esetben nem közvetlenül okoznak kárt, hanem csak elindítják az ahhoz vezető eseményeket. Brenner szerint azonban egy atomerőmű felrobbantására senki sem számítógépes terrorizmusként, hanem inkább nukleáris terrorizmusként emlékezne.[54]

A tömeges zavarkeltés fő célja a lakosság biztonságérzetének aláásása a kormányzatba vetett bizalom lerombolásának segítségével. Brenner szerint ilyen eredménnyel járhat, ha például egy hagyományos terrorcselekmény elkövetésének időpontjában mértékadó médiák weboldalait feltörik és azokon hamis információkat terjesztenek, vagy hamis közleményeket tesznek közzé kormányzati oldalakon. Ugyan ennek a pánikkeltő hatása erősen korlátozott, mégis növelheti a zavart a hagyományos támadás miatt egyébként is pszichológiai nyomás alatt lévő lakosság körében.[55] Ezzel a felhasználással kapcsolatban aggodalomra adnak okot az elmúlt évek álhírekkel kapcsolatos fejleményei, különösen például a 2016-os amerikai elnökválasztás tapasztalatai. Ugyan az álhírek terjesztése alapvetően a korábban már érintett propagandatevékenységet jelenti, az így elterjesztett hamis információknak súlyosabb társadalmi következményei is lehetnek, például abban az esetben, amikor egy amerikai férfi lövöldözni kezdett egy helyi pizzériában, mivel elhitte, hogy az valójában egy titkos gyerekmolesztáló hálózat része.[56]

A társadalmi rend szétzilálása esetén az elkövetők fő célja, hogy a civil lakosság társadalom működésébe vetett hitét rombolja, például közműszolgáltatások vagy más kritikus infrastruktúrák leállításával. Ebben az esetben nem a rendszerekben történő közvetlen károkozás a cél, hanem a társadalmi bizalom lerombolása.[57] Ugyanakkor ennek a gyakorlati hasznossága annyiban kérdéses, hogy például áramkimaradások terrorcselekményektől függetlenül is történnek, például 2005-ben öt-

[54] Brenner: i. m. 453–471. o.
[55] Brenner: i. m. 453–471. o.
[56] https://www.reuters.com/article/us-washingtondc-gunman/man-pleads-guilty-in-washington-pizzeria-shooting-over-fake-news-idUSKBN16V1XC [2018.06.23.]
[57] Brenner: i. m. 453–471. o.

ven millió amerikai maradt áram nélkül, így csak az igazán kirívó eseteknek lehet érezhető társadalmi hatása.[58]

6. Valós a fenyegetés?

Mint CONWAY nyomán GILLESPIE is rámutat, a kiberterrorizmus koncepciója a terrorizmustól és a technológiától való félelmet testesíti meg. A múltban a hackertámadásoktól való félelem volt képes hasonló reakció kiváltására, és néhányan odáig merészkednek, hogy „ítéletnapi forgatókönyveket" vázoljanak fel. A legsebezhetőbb kritikus infrastruktúrák – mint például a bankrendszer vagy az áramellátás – azonban nem kapcsolódnak az internethez, és így jóval nehezebb ezeket célzó kibertámadást indítani.[59] Azonban nem lehetetlen, mint azt a Stuxnet példája is mutatja, hiszen az iráni urándúsító üzem is internetkapcsolat nélkül működött, amit a beszállítók megfertőzésével tudtak megkerülni. Ugyanakkor a problémát hajlamosak sokan túlbecsülni, és az érzelemtől fűtött retorikát összekeverni a valóságos lehetőségekkel, ami egyébként is komoly probléma a kiberbűnözéssel kapcsolatos kommunikáció terén.[60] STOHL véleménye szerint a kiberterrorizmussal kapcsolatos fő aggályok a félelemből és tudatlanságból erednek.[61] MEZEY véleménye szerint a félelem mellett a bizonytalanság, a média szenzációhajhászása is a veszély túlbecsüléséhez vezettek.[62]

Csakugyan tény, hogy napjainkig egyetlen olyan jelentős kibertámadásra sem került sor, amit terrorszervezetek hajtottak volna végre. GILLESPIE abban látja a kiberterrorizmus elterjedésének fő gátját, hogy az egyszerűen nem elég „látványos" ahhoz, hogy a megfelelő hatást kiváltsa. Például egy áramkimaradás okozása nem jár olyan tömeglélektani hatásokkal, mint egy robbantás egy forgalmas helyen. Ráadásul a fizikai világban, még ha nem is sikerül egy támadás, úgy is képes zavart okozni, például egy forgalmas pályaudvar lezárásával. Ezzel szemben egy sikertelen kibertámadásnak aligha lehet ilyen hatása, sőt a célpont talán meg sem tudja, hogy támadást kíséreltek meg ellene.[63]

[58] GILLESPIE: i. m. 109. o.
[59] GILLESPIE: i. m. 108. o.
[60] WALL: i. m. 26–27. o.
[61] CASSIM: i. m. 387. o.
[62] MEZEY: i. m. 46. o.
[63] GILLESPIE: i. m. 109. o.

7. Válaszok a kihívásra

A kiberterrorizmussal kapcsolatos nemzetközi és állami válaszok szorosan összefüggnek a terrorizmusra adott válaszokkal, és azok nehézkes és kiforratlan rendszerével. Az ott meglévő problémák ennél a jelenségnél még élesebben kiütköznek, a kiber elemből fakadó jellemzőknek köszönhetően. A terrorizmussal nemzetközi egyezmények rendszere meglehetősen kusza, és szinte teljes egészében nemzeti hatáskörbe utalja a terrorizmus elleni fellépést, amely igen sok esetben nem vezet eredményre (politikai akarat hiánya, bukott államok), így pedig a szankció sem bír olyan elrettentő erővel.[64] A terrorizmus elleni küzdelem jelenlegi nemzetközi rendszere tehát nem olyan, amire támaszkodni lehetne a kiberterrorizmussal szemben. Ígéretesebb azonban a kiberbűncselekményekkel kapcsolatos szabályozás: a legszélesebb körben elfogadott egyezmény az Európa Tanács 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye, amely számos minimumszabályt tartalmaz a büntető anyagi és eljárási jog területén.

Anyagi jogi szempontból – mint arra már a fogalom kapcsán is kitértem – az EU terrorizmus elleni küzdelemről szóló 2017/541 irányelve már előírja a tagállamok számára, hogy a terrorizmus részeként kriminalizálják a kiberterrorizmust. Az Egyesült Királyságban a 2000. évi terrorizmusról szóló törvény bünteti az olyan támadásokat, amelyek az elektronikus rendszerekbe történő súlyos beavatkozásra vagy zavarásra irányulnak.[65] Ettől eltérő módon az Egyesült Államokban 2001-ben elfogadott hazafias törvény (PATRIOT Act) a kiberbűncselekmények között szabályozta a kiberterrorizmust. Ugyanígy a kiberterrorizmus elleni fellépést szolgálta az Obama elnök által 2015. április 1-jén aláírt 13694. számú elnöki rendelete, amelynek hármas célja volt, így a „rosszindulatú kiberszereplők" vagyonának zárolása; megakadályozni, hogy pénzhez jussanak; illetve belépésüket az Egyesült Államok területére. Azonban alkalmazására egyetlen alkalommal került csak sor, Oroszországgal szemben a 2016-os elnökválasztás befolyásolása miatt, ami alapvetően megkérdőjelezi, mennyire hasznos a kiberterrorizmus visszaszorításában.[66]

Eljárásjogi szempontból[67] a legkomolyabb problémák egyike az internet globális jellegéből fakad, és az ebből eredő joghatósági kérdésekből. A jelenlegi terrorizmus

[64] Dornfeld – Sántha: i. m. 99–100. o.

[65] Cassim: i. m. 390. o.

[66] Brunner, Jordan A.: The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergeny. Jurimetrics, 2017/3. 398. o.

[67] Lásd kriminalisztikai aspektusok vizsgálatát Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8. 441-443. o.

elleni egyezmények az aut dedere aut judicare elvet vallják a magukénak, ám a hagyományos terrorizmussal szemben itt nem ismert az elkövető személye, így szintén nem alkalmazható. A kiberbűnözéssel kapcsolatos joghatósági kérdések vonatkozásában szupranacionális szinten, az EU-s joganyagban találunk iránymutatást. Az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv[68] 12. cikke az elkövetés helyét, illetve az állampolgárságot határozza meg, mint joghatósági okok, de lehetőséget ad a tagállamoknak, hogy megállapítsák joghatóságukat, ha a területükön található jogi személy javára történt az elkövetés, vagy pedig az elkövető szokásos tartózkodási helye a területükön van. Komoly hiányosság azonban, hogy az irányelv nem állapít meg sorrendiséget ezen joghatósági okok között, így lényegében a tagállami szerveknek kell erről megegyezniük. Akárcsak a terrorcselekményeknél, a kiberterrorizmusnál is az egyik legjelentősebb előrelépés az univerzális joghatóság megállapítása lenne.

A vizsgálódást a terroristák egyéb internetes tevékenységével kapcsolatos reakciókra is kiterjesztve megállapítható, hogy ezen a téren is szigorításokra került sor. Így például a Twitter a felületén az Iszlám Állam által kifejtett jelentős propagandatevékenységének visszaszorítására szigorított az addigi politikáján, ami komoly felületvesztéssel járt a szervezet számára.[69] Szabályozási szinten is számos törekvés született azzal kapcsolatban, hogy felléphessenek a terrorista tartalmat terjesztőkkel szemben. Számos államban, így például az Egyesült Királyságban, Spanyolország és Franciaországban bűncselekménnyé vált a „terrorizmus dicsőítése". A magyar jogrend a Btk. 331. § (2) bekezdés alapján háborús uszításként kriminalizálja a „nagy nyilvánosság előtt a terrorizmus támogatására uszítást, vagy egyébként a terrorizmust támogató hírverés folytatását". Hasonló úton jár az EU terrorizmus elleni küzdelemről szóló 2017/541 irányelve, amelynek 5. cikke szintén előírja a tagállamoknak a terrorcselekmények elkövetésére buzdító magatartások, így például a terrorizmus dicsőítésének kriminalizációját. Sokan azonban a gyakorlattal szemben foglalnak állást, például Ben Emmerson ENSZ különmegbízott is, aki a homályos megfogalmazásból eredő, és a szólásszabadságot potenciálisan korlátozó problémákra helyezi a hangsúlyt.[70]

Komoly erőfeszítések figyelhetők meg a titkosítás szabályozása terén is. Számos államban bűncselekménnyé vált megtagadni a titkosítást feloldó kulcs átadását a hatóságok számára.[71] A belga büntetőtörvénykönyv egy, míg a francia 434-15-2. szakasza három, illetve minősített esetben öt évig terjedő szabadságvesztéssel rendeli büntetni azt, aki meg-

[68] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. HL 2013 L 218., 2013.8.14.
[69] Besenyő: i. m. 161. o.
[70] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17229 [2018.06.23.]
[71] Gillespie: i. m. 111. o.

tagadja a feloldáshoz szükséges kulcs átadását a hatóságoknak. Nagy-Britanniában a 2000. évi vizsgálati hatáskörök szabályozásáról szóló törvény 53. szakasza nemzetbiztonsági és gyermekeket érintő ügyekben 5 évig, egyéb estekben 2 évig terjedő szabadságvesztést helyez kilátásba, ha valaki megtagadja a titkosítást feloldó kulcs átadását. Ez azonban elég komoly aggályokat vet fel, és az önvádra kötelezés tilalmába ütköző lehet. Támogatói úgy érvelnek, hogy nem maga kulcs a terhelő, hanem az azzal védett információk, ilyenformán ez egy semleges adatnak tekintendő, akárcsak a vér vagy DNS minta.

Hazánkban a terrorellenes intézkedések részeként született meg a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről szóló 185/2016. (VII. 13.) Kormányrendelet, amely előírja az alkalmazásszolgáltatóknak, hogy nem hajthatnak végre olyan fejlesztéseket, amelyek a titkos információgyűjtést kizárják vagy ellehetetlenítik. Ennek hatásai ugyanakkor kétségesek, hiszen az elkövetők számos külföldi fejlesztésű eszközt beszerezhetnek, amelyek fejlesztőire ezek a rendelkezések nem vonatkoznak. Elég csak egy egyszerű iPhone-ra gondolni, amelyen hamarosan bezárják az eddigi biztonsági réseket a fejlesztők, így a bűnüldöző és terrorelhárítási szervek sem ismerhetik meg a rajtuk tárolt adatok tartalmát.[72]

Összefoglalás

A kiberterrorizmus kapcsán igen élénk diskurzus folyt nemcsak a jogtudományban, de a médiában és a társadalomban is az elmúlt évtizedekben. A 2001-es terrortámadásokat követően sokan tartottak attól, hogy a terrorizmus könnyedén új erőt meríthet a kibertér kiaknázásából, és a terroristák ezen keresztül indíthatnak újabb és még pusztítóbb támadásokat. A jelenséggel kapcsolatban hamar a pesszimista hangok váltak uralkodóvá, például az Egyesült Államok 2002-es kiberbiztonsági gyakorlatát „digitális Pearl Harbor" névre keresztelte, míg hazai vonatkozásban a „digitális Mohács" kifejezés jelent meg.[73] Az új technológia jelentette veszélyek már régóta mozgatják az emberek fantáziáját, és az ezektől való félelem számos film, könyv, videojáték témájává is vált.

A 2001. szeptember 11. óta eltelt években mind a mai napig nem került sor jelentős kiberterrorista támadásra sehol a világon, ami véleményem szerint azt mutatja, hogy a jelenséggel kapcsolatos félelmek túlzóak voltak. Ugyan képes lehet egy

[72] https://apnews.com/8b23b35b73684c3d90f739c90949146f/Apple-closing-iPhone-security-gap-used-by-law-enforcement [2018.06.23.]

[73] Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. 2010/2.

csoport egy állam digitális működésében súlyos fennakadásokat okozni, mint Észtország esetén 2007-ben az orosz hackerek, ennek lélektani hatása korántsem azonos egy terrorcselekményével. Észtország esete korántsem vált ki olyan erős érzelmi reakciót, mint a New York-i ikertornyok leomlását bemutató képek, hiszen előbbi jóval megfoghatatlanabb, mint a fizikai rombolás. Így bár elméletben a kiberterrorizmus sokkal jelentősebb veszély a hagyományos terrorizmusnál, a valóság egyelőre látványosan nem kíván igazodni ehhez a felvetéshez. A terrorizmus jövőbeli tendenciáit vizsgáló kutatások is elsősorban a hagyományos eszközökkel elkövetett terrortámadások számának további növekedésével számolnak.[74]

A kiberterrorizmus kapcsán alkalmazható az a régi mondás, hogy „jobb félni, mint megijedni", vagyis az államoknak készen kell állniuk arra, hogy megvédjék polgáraikat a kibertérből érkező terrorfenyegetésekkel szemben. Napjainkra egyre több jogrendszer kriminalizálta a kiberterrorizmust – vagy a kiberbűnözés vagy a terrorizmus részeként –, és a kibervédelmet ellátó szervek és incidenskezelő központok is egyre hatékonyabban működnek. Jelenleg az állami támadások a leginkább jellemzők, amelyek célja vagy a kémkedés vagy az ellenfél védelmének tesztelése.

A kiberterrorizmusról szóló diskurzus kapcsán sokszor kevéssé kap helyet a terroristák egyéb internetes tevékenységének vizsgálata, amely talán a legkomolyabb negatív hozadéka a kiberterrorizmus veszélyessége túlértékelésének. Ezek jóval kevésbé ijesztő tevékenységek, mint például egy erőmű felrobbantása, de véleményem szerint jóval veszélyesebbek. Az elmúlt évek nyugat-európai terrortámadásaiban jelentős szerepet játszott a terroristák internetes kommunikációja, az aktív dzsihadista propaganda és persze azok a pénzügyi támogatások, amelyeket a terrorszervezetek az internet segítségével szereztek meg. Véleményem szerint ez egy olyan téma, amivel szemben a jövőben még keményebben kell fellépnie a nemzetközi közösségnek.

Felhasznált Irodalom

Berki Gábor: Kiberháborúk, kiberkonfliktusok. In: Pintér István (szerk.): A virtuális tér geopolitikája. Geopolitikai Tanács, 2016.

Besenyő János: Az Iszlám Állam. Terrorizmus 2.0. Kossuth Kiadó, Budapest, 2016.

Bozonelos, Dino – Stocking, Galen: The Effects of Counter-Terrorism on Cyberspace: A Case Study of Azzam.com. Journal of the Institute Of Justice & International Studies, 2003/3.

[74] Ritecz György – Sárkány István: A jövő terrorizmusa. Belügyi Szemle, 2013/6. sz. 22. o.

BRENNER, W. Susan: Cybercrime, Cyberterrorism and Cyberwarfare. Revue internationale de droit pénal, 2006/3.
BRUNNER, Jordan A.: The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergeny. Jurimetrics, 2017/3.
BUONO, Laviero: Gearing Up the Fight Against Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). New Journal of European Criminal Law, 2012/3.
CASSIM, F.: Addressing The Spectre of Cyber Terrorism: A Comparative Perspective. Potchefstroom Electronic Law Journal, 2012.
DENNING, D. E. : Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In: J. Arguilla, D. Ronfeldt (ed.) = Networks and Netwars: The Future of Terror, Crime, and Militancy. 2001.
DORNFELD László – SÁNTHA Ferenc: A terrorizmus és a terrorcselekmény, mint nemzetközi bűncselekmény aktuális kérdései. Jog Állam Politika 2017/3.
EICHENSEHR, Kristen E.: The Cyber-Law of Nations. Georgetown Law Journal, 2015/2.
Environmental Risks: Cyber Security and Critical Industries.
FENYVESI Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8.
GILLESPIE, Alisdair A.: Cybercrime – Key Issues and Debates. Routledge, 2016.
GYARAKI Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012.
HOLT, Thomas J. – BOSSLER, Adam M. – SEIGFRIED-SPELLAR, Kathryn C.: Cybercrime and digital forensics: An introduction. Routledge, 2018.
HUMMEL, Michael L.: Internet Terrorism. Homeland Security Review 2/2008.
ILLIG, A. T.: Computer Age Protesting: Why Hacktivism is a Viable Option for Modem Social Activists. Penn State Law Review, ?/2015.
KISS Attila: A privátszférát erősítő technológiák. Infokommunikáció és jog 2013/56.
KOVÁCS László – KRASZNAY Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. 2010/2.
LUKÁCSI Tamás: A terrorizmus elleni küzdelemről szóló (EU) 2017/541 európai parlamenti és tanácsi irányelv. Európai Jog 2017/6.
MARAS, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017.
MATUSITZ, Jonathan: Terrorism & Communication. A Critical Introduction. Thousand Oaks, SAGE Publications, 2013.
MEZEI Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1.

MEZEY Nándor Lajos: Kiberterrorizmus: valós veszély? Belügyi Szemle, 2011/2.
NAGY Zoltán – MEZEI Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog. 2018/70.
NAGY Zoltán András – MEZEI Kitti: A zsarolóvírus és a botnet vírus, mint napjaink két legveszélyesebb számítógépes vírusa. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Pécsi Határőr Közlemények XIX. Pécs, 2017.
NAGY Zoltán András – MEZEI Kitti: The organised criminal phenomenon on the Internet. Journal of Eastern-European Criminal Law. 2016/2.
NAGY Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula – Hautzinger Zoltán: Pécsi Határőr Tudományos Közlemények XIII. 2012.
OLEKSIEWICZ, Izabela: Dilemmas and Challenges for EU Anti-Cyberterrorism Policy: The Example of the United Kingdom. Teka Kom. Politol. Stos. Międzynar. 2016/3.
PARTI Katalin: Kerekasztal-beszélgetés az online terrorizmusról. Ügyészek Lapja, 2010/2.
PATAKI Márta – KELEMEN Roland: Kiberterrorizmus. A terrorizmus új arca. Magyar Rendészet 2014/5.
PINTÉR István: A virtuális tér geopolitikája. In: PINTÉR István (szerk.) A virtuális tér geopolitikája. Geopolitikai Tanács, 2016.
RITECZ György – SÁRKÁNY István: A jövő terrorizmusa. Belügyi Szemle, 2013/6. sz.
SIMON Béla: Hacktivism and Its Status in Hungary. Magyar Rendészet 2016/2.
SIPOS Zoltán: A kibertér biztonságával kapcsolatos alapvető kérdések áttekintése. Honvédségi Szemle, 2016/1.
SZATHMÁRY Zoltán: Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban. PhD értekezés. Budapest, 2012.
TROPINA, Tatiana: Fighting money laundering in the age of online banking, virtual currencies and internet gambling. ERA Forum, 2014/1.
WALL, David S.: Cybercrime: The Transformation of Crime in the Information Age. Polity, 2007.
WARREN, M. J.: Terrorism and the Internet. In: JANCZEWSKI, Lech J. – COLARIK, Andrew M. (ed.): Cyber Warfare and Cyber Terrorism. Information Science Reference, 2008.

FENYVESI CSABA

KRIMINALISZTIKAI VILÁGTENDENCIÁK – KÜLÖNÖS TEKINTETTEL A DIGITÁLIS FELDERÍTÉSRE

Ha áttekintjük a kriminalisztika, a modern bűnüldözés tudomány elmúlt, mintegy 120-170 évét, és figyelembe vesszük a mérföldköveit, a tudományfejlődés tendenciáit, a paradigmaváltásokat és a bizonyítékok generációs változásait akkor – nézetem szerint – az alábbi világtendenciák rajzolódnak ki napjainkban.[1]

1. A krimináltechnika elsődlegesssége (primátusa)
2. Specializálódás
3. Minúcializálódás (mikroszkopizálódás, miniatürizálódás)
4. A múlt közeledése – a képek élesedése
5. Expertizálódás („szakértősödés")
6. Valószínűségi szint erősödések
7. Csapatmunka dominancia
8. Komputerizálódás („számítógépesedés")
9. Cyberfelderítés („digitkommandó") előretörése
10. Titkos eszközök és módszerek felértékelődése
11. Nemzetköziesedés (internacionalizálódás)
12. Veszélyhelyzetek szaporodása
13. Privatizálódás (magánosítás)

Tanulmányom címéből látható, hogy legszorosabban a 9. tendencia kötődik a jelen kötet témájához, ám kisebb-nagyobb áttételeken keresztül szinte mindegyiknek van kapcsolata a XXI. századi digitális felderítéshez, az elektronikus adatokhoz, illet-

[1] Korábbi kutatásom során utaltam már néhány tendenciára ezek közül, ám most a „A bűnügyi tudományok és az informatika" című kötet keretében bővíteni tudom és tovább részletezhetem célirányosan, illetve újra fogalmazhatok néhány jelenséget. Lásd a korábbiakról: Fenyvesi Csaba: A XXI. századi bűnüldözés-tudomány nemzetközi tendenciái. Magyar Tudomány, 2004/6. 757-765. o., illetve: A kriminalisztika XXI. századi világtendenciái. Belügyi Szemle, 2013/10. 7-33. o.

ve az elektronikus bizonyítékokhoz[2], ahogyan a 2018. július 1-től hatályba lépő új 2017. évi XC. törvény fogalmazza büntetőeljárásról. Így nem haszontalan és érdektelen néhány szót ejteni az egyéb világtendenciákról sem. Mellőzve a lista végén szereplő, a témától némileg távol álló veszélyhelyzetek szaporodását és a privatizálódást.

1. A krimináltechnika elsődlegessége (primátusa)

A) A tendenciák között is első helyre helyezem a krimináltechnika primátusát, ami kötődik a digitális adatokhoz, hiszen ezek is technikai jellegűek.

Úgy vélem, hogy még a kriminalisztika különös részébe tartozó, egyes bűncselekmények speciális felderítési ajánlásairól szóló kriminálmetodikánál is a krimináltechnikai irányvonal erősödik, semmint a krimináltaktikai. Lévén, hogy maguk a bűncselekmény elkövetési formák is sokszor technikai jellegűvé váltak és válnak. Például a digitális adatokhoz szorosan kötődő bankkártya csalások,[3] gépmanipulációk, foglalkozási szabályszegések.

B) A bűnüldözés-tudomány a bűnügyi tudományok rendszerében már gyökereitől, a XX. század elejétől fogva különleges helyzetet foglal el. Egyfelől egy nagyon gyakorlatias, alkalmazásorientált tudomány, amelynek pontos terjedelme és tartalma az eltelt kb. másfél száz év alatt is folyamatosan vitatott, másfelől a tudományággal kapcsolatos tudásanyag növekvő mértékben és egyre nagyobb sebességgel változik. Ez a változás legfőképpen a természettudományi ismeretekre alapozódó krimináltechnika – azon belül is a számítógép, a kibertechnika által támogatott felderítés – esetében szembetűnő és szinte mindennapos. Ilyen mérvű haladásról, „forradalomról" és paradigmaváltás(ok)ról – a főleg társadalomtudomány eredményeire épülő kriminálta ktikánál – nem beszélhetünk, és ez a jövőben sem várható az alaptudományok jellege miatt.

C) Azt is elvi éllel mondhatom ki a kriminálta ktikai felhasználási ajánlások és alkalmazások teljes körének áttekintése alapján, hogy javarészük napjainkban már kriminálta chnikai, de legalább technikai alapokra épül.

Elsőként kiemelhető, mint ahogyan az életben is általában elsőként történik meg, az alapos, szakmailag igényes, XXI. századi helyszíni szemle, amelynek során

[2] Lásd bővebben: Gaál Tibor: A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban. Belügyi Szemle 2018/7-8. 22-35. o.

[3] Mezei Kitti – Tóth Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós – Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017. 297-308. o.

a nyomok és – sokszor szabad szemmel nem látható, látens – anyagmaradványok, mostanság pedig a digitális (számítógépes) adatok felkutatása, rögzítése, biztosítása és vizsgálata széleskörű technikai bázisra, eszközrendszerre és metódusra épül. Csakúgy mint egy modern házkutatás, amelynek lefolytatásakor a legkorszerűbb kereső eszközök, technikai berendezések (detektorok, UV-lámpa, a virtuális házkutatáshoz pedig számítógépek, kémprogramok stb.) állnak a gyakorta speciális tárgyat (aranyat, fémes elkövetési eszközt, kábítószert, uránt, hamis pénzt, digitális adatot stb.) vagy szökésben levő, rejtőző embert kereső bűnüldözők rendelkezésére. Ám ide sorolhatjuk a bizonyítási kísérleteket is; ezeknél a legfőbb kérdés mindig az eredeti, bűncselekménykori állapothoz legközelebb álló, optimális esetben azonos körülmények megteremtése. Ez alapvetően szintén technikai kérdés és csak erre épülhet valamiféle kriminál taktika. Még a napjainkban újdonságnak ható profilalkotási módszer vagy a bűnelemzés mögött is hallatlan technikai apparátus rejlik az adatok rendszerezése, a komputerizált feldolgozás következtében.

Majdhogynem az marad igazán kriminál taktikai módszertan, ami – feltehetően – sohasem lesz felcserélhető technikával a jövőben sem, legfeljebb segíthető (pl. számítógéppel), a nyomozás tervezése, szervezése, irányítása, az adatok rendszerezése, analízise és szintézise, végső soron a gondolkodás. Valamint, ami széppé, izgalmassá teszi a tudományág művelését, az intuíció, a bele- és megérzés, a megsejtés misztikuma, a szenvedéllyel és emberi érzelmekkel, ugyanakkor racionalitással is teli, sokszor a véletlent is kihasználó bűnüldözés.

D) A jelen századra egyértelművé vált, hogy a szervezett bűnözés a legnagyobb kihívás a bűnüldözés számára. Területei szinte felölelik a mindennapi élet összes szektorát. Kiemelkedő helyet tölt be a kábítószer- műkincs- fegyver- prostitúciós- és emberkereskedelemben, pénzmosásban, kalózkodásban, valamint a cyber és terrorista (bűn)cselekedetek végrehajtásában.[4] Megfigyelhető jelenség, hogy ezzel párhuzamosan a sértetti kör mintegy elszemélytelenedik, elmosódik az egész bolygóra kiterjedő hatalmas tömegben, ami csökkenti a kriminál taktikai elemek bevetésének lehetőségét. A szervezett elkövetés – mint ahogyan megnevezéséből is látható – jól szervezett, kimunkált, technikailag is erőteljesen támogatott, magas szintű. Ezzel szemben hatékony megelőzést, illetve felderítést is csak magas szintű technikai apparátussal lehet folytatni, amelynek domináns része titkos eszközöket jelent. A műholdas követő rendszeren keresztül, az egész világot lehallgatni képes,

[4] Egyesek „krízis szituációnak" és egyúttal kihívásoknak nevezik a terrorista cselekedeteket a bűnüldözés szempontjából. KORAJLIC, N., – TEOFILOVIC, N. – KESETOVIC, Z.: Terrorist act as crisis situation – challenge for investigators. In: NBP Journal of Criminalistics and Law. Kriminalisticko-Policijska Akademia, Beograd, 2009. 123-133. o.

épületeket, személyeket átvilágító és rögzítő készülékek mind technikai csúcsteljesítmények, amelyek nélkül nem lehet sikeres korunk bűnüldözése.

E) Felfogásom szerint a bűnüldözés-tudomány eredményessége a tárgyalótermekben dől el, ott a végső „eredményhirdetés." A tapasztalatok azt mutatják, hogy a civilizált világ minden pontján a „megvásárolhatatlan tanúk", a tárgyi bizonyítékok, a nyomok és anyagmaradványok tudományos megalapozottságú hitelt érdemlősége a legfontosabb bizonyíték, a bűnüldözés „aduja". (Jóval kisebb a százalékos hibaforrás aránya, mint a személyi bizonyítékú felismerésre bemutatásnak és vele szimbiózisban a tanúvallomásnak.) A tárgyi bizonyítékok pedig természettudományi ismeretekre, hallatlanul elmélyült és sebesen fejlődő tudásra, kutatási tapasztalatra, tudományos ismérvrendszerre épülnek. Amilyen mértékben fejlődnek a természettudományi „anyatudományok" (biológia, fizika, kémia, matematika, informatika, kibernetika stb., és ezek alágai) olyan mértékben – némi, néhány éves, de mindenképpen egyre rövidülő késéssel átvéve – fejlődik (a legfőképpen) adaptáló tudományok körébe tartozó kriminalisztika is.

2. Specializálódás

A) A bűnüldözés-tudomány elmúlt másfélszáz éve alatt annyi ismeret halmozódott fel, hogy egyáltalán nem túlzó állítás, hogy nincs olyan személy, aki ma minden alkalmazott kriminál technikai és taktikai metódust ismerne, vagy akár birtokolna. Ahogyan a szintén rohamosan fejlődő alkalmazott tudományban, az orvostudományban is fikció az „orvos" kifejezése, úgy a bűnüldözés-tudományban sincs polihisztor szintű „kriminalista". Legfeljebb egy-egy területre, egy-egy tudományos „mezőre", sávra rálátó, abban szakértőként résztvevő személyekről beszélhetünk. Ilyen „mezők" lehetnek a bűnüldözés-tudományban:

   a) traszológián belül: ujj, tenyér, tenyérél, láb, lábbeli, ajak, homlok, fül, fog, fém, fémbeütés, közlekedési eszköz, egyéb eszköznyom;
   b) anyagmaradványok körében: szag,[5] haj, szőr, textil, vér, vizelet, ondó, izzadság, nyál, csont, egyéb emberi anyagmaradványok, állati és növényi anyagmaradványok, festék, üveg, talaj, műanyag, fém, gyertya, por, kábí-

[5] Lásd erről részletesebben: Horváth Orsolya: Az emberi szag jövőbeni kutatásának lehetőségei és korlátai. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2013. 395-399.o., illetve: Szolgálati kutyák a rendvédelemben: a múlt, a jelen és a jövő lehetőségei. Magyar Rendészet, 2015/3. 59-71. o.

tószer (már azon belül is alcsoportok), ásvány, egyéb szerves és szervetlen anyagok, bogár-rovar, DNS-azonosítás;

c) egyéb kriminál technikai metódus körében: okmány-, pecsét-, bélyegző-, hologram-, írás-, gépírás-, aláírás-, nyomtatóírás-, festmény-, fegyver-, lőszer-, robbanószer-, tűzvizsgálat, hangazonosítás, személyazonosítás, poligráf, számítógép-azonosítás, számítógép nyomtatóazonosítás, számítógépfeltörés-elhárítás, számítógépvírus-elhárítás, virtuális-digitális adatgyűjtés, fénykép-videóazonosítás, tervezési-építési balesetek vizsgálata (engineering failure);

d) kriminál taktika körében: nyomozás tervezés-szervezés-logisztika-management, helyszíni szemlézés, (földrajzi) bűnözés-elemzés (crime analysis), bűnelkövetői profilalkotás (criminal profiling), viselkedéstudomány, (behavioral science), sértett-gondozás (forensic nursing), kihallgatási taktika, köztük a kognitív interjú vagy az angol SAI-modell (Self Administered Interview).

B) A felsorolásból is kitűnik, hogy a megváltozott tudásmennyiség által kikényszerített specializálódás megy végbe, amelynek keretében a bűnüldözés-tudomány képviselői vagy a vizsgálat tárgya és/vagy módszere alapján néhány területen mozognak, kutatnak, adnak szakvéleményt. Minél magasabb szintűvé, minél elmélyültebbé válnak az adott részterület tudományos ismeretei, módszerei, annál inkább szűkül az egy személy által a század követelményeinek megfelelően, megbízhatóan művelhető egységek (sávok és mezők) száma, egyúttal annál magasabb szintűvé is válik egy-egy képviselő produktuma. A folyamat megállíthatatlanul a minimális egységszám, az egy felé közelít. Egyre inkább csak igen szűk területen, azon belül azonban széles skálán és nagy precizitással képesek és alkalmasak a bűnüldözés-tudomány szakemberei biztos válaszokat nyújtani a kriminalisztikai fő kérdésekre.

3. Minúcializálódás (mikroszkopizálódás, miniatürizálódás)

Az előző két pontban foglaltakkal van szinkronban, hogy a szélesebb értelemben vett bűnüldözés számára egyre nagyobb jelentőséggel bírnak a bűncselekményhez, illetve az elkövetőhöz kötődő nyomok és anyagmaradványok. Világtendencia – véleményem szerint –, hogy miközben egyre fejlettebb a bűnfelderítési technika, ezzel ellentétes irányban mozog a bűnelkövetők által hagyott, ejtett nyomok, anyagmaradványok mennyisége és minősége. Vagyis a minél fejlettebb kriminál-

technikával szemben egy egyre inkább kvalifikációt mutató bűnelkövetési módszertan is kialakult. A bűnüldözés szomorú ténye, hogy valóban, mint ahogyan az elnevezése is mutatja: „üldözés". Ez szükségszerűen egy követő magatartást feltételez, így a bűnüldözés-tudomány képviselői mindig a bűnelkövetők mögött járnak. A kriminál technikai módszerek sem előzik meg a bűnelkövetési módokat, kivéve a proaktív eszközök kis csoportját. Úgy is fogalmazhatok, hogy a bűnelkövetési módszertan – és ebbe beleértendő a digitlizáció is – ez idáig fejlettebb, gazdagabb volt, mint a bűnfelderítési.[6]

Ebből adódóan a világ kriminál technikai eszköztárának bővülésével, jelentős fejlődésével egyidejűleg, ellentétes tendenciaként a bűncselekményekkel kapcsolatos nyomok-anyagmaradványok csökkenését, szűkülését tapasztaljuk. Az igazságszolgáltatás – mint szélesebb körben értelmezett bűnüldözés – szemszögéből vizsgálva úgy is megfogalmazhatjuk Tremmel Flórián szavaival, hogy „bizonyítékínség" van az eszközbőséggel szemben.[7] A bizonyítékínségben felerősödnek a nem látható, miniatürizált nyomok és anyagmaradványok, amelyek jelentősége egy-egy ügy felderítésében, megítélésében perdöntő lehet. Ilyen nem látható, csak mikroszkóppal vagy ehhez hasonló „feltáró", a külvilág számára értékelhetővé tevő eszközzel nyilvánosságra hozott, a büntetőeljárásba bekapcsolt, felkutatott, rögzített, majd azonosított minúciáknak, apróságoknak felértékelődött és még inkább felértékelődik a szerepük. (Példaként említjük csak meg a DNS sejtmagot tartalmazó, helyszínen hagyott bőr-nyál-izzadtságcseppeket.)

4. A múlt közeledése – a képek élesedése

Szoros összefüggés van az előző ponttal, mivel éppen a miniatűr nyomok, anyagmaradványok alapján nézünk a múltba. Mivel szükségszerűen múltbeli eseményeket vizsgál a kriminalisztika, ezért a „távolba látás" képessége, a távoli képek „élesítése" állandó kívánalom és követelmény. Ennek a követelménynek – úgy tűnik – egyre inkább, mondhatjuk tendenciózusan megfelel a kriminalisztika módszertana, eszköztára. Állíthatjuk, hogy minél közelebbi a múltbéli kép, annál távolabbi lesz a nyom nélküli, tökéletes elkövetés tettesi álma. A következő esettanulmányokkal és módszerekkel erre a jelenségre kívánunk rávilágítani.

[6] Lásd erről részletesebben: Tremmel Flórián – Fenyvesi Csaba – Herke Csongor: Kriminalisztika. Dialóg Campus Kiadó, Budapest-Pécs, 2005.

[7] Tremmel Flórián: Magyar büntetőeljárás. Dialóg Campus Kiadó, Budapest-Pécs, 2001. 207-224. o.

Az 1991-ben az osztrák-olasz Alpok egyik gleccserében, kellő hűtéssel konzerváltan és relatíve jó épségben megtalálták – a felbukkanási helyéről elnevezett – „Ötzi" ember maradványait, csontvázát, ruházatát, használati tárgyait. Éppen a kriminalisztika módszertanában használt eszközökkel, ténykutatási szakértői módszerekkel vizsgálták meg az elmúlt 20 évben, több alkalommal különböző expertológus csapatok. Mindannyiszor egyre többet tudtunk meg róla. Mindenekelőtt, hogy a 45-46 évesen meghalt férfi 5300 éven át feküdt természetes sírjában, vadászó életmódot folytatott, 159 centiméterre nőtt, 40 kilós – epeköves, ízületes, jó fogazatú – testét gabonamagokkal és szarvas, illetve kecskehússal táplálta. Végül, hogy kriminális esetről beszélhetünk vele kapcsolatban is: az anyagmaradványok üzenete szerint megölték, hátulról lenyilazták. A második nagy vizsgálatnál megtalálták a – „kiirthatatlan" – végzetes nyílhegy darabkát a hátrészén, szilárdan és mélyen beékelődve a csontozatba.

5. Expertizálódás („szakértősődés")

A) A kriminál technika szédületes tempójú fejlődése mögött az „éleslátással" (többek között az elkövetői komputerek agyába is nézve) felszínre hozott (digitális) nyomok és anyagmaradványok vizsgálata áll, márpedig ezt már laikus, egyszerű nyomozói képességekkel és tudással nem lehet szakszerűen elvégezni. Specialistára van szükség, hogy a „néma tanúk" megszólaljanak, hogy laboratóriumi körülmények között mindent elmondjanak. Egyre szaporodnak az olyan ügyek, amelyeknél elengedhetetlen a magas minőségű szaktudás, például a tárgyi bizonyítékok felkutatásához és különösen a „vallatásukhoz".[8] Tendenciózusan egyre több eset van, amelynél mindenképpen ott kell lennie, részt kell vennie valamilyen szakértőnek, „expertnek" („expert witness"-nek). A helyszíni szemlék sokasága sem folytatható le (már) jelenlétük nélkül. A legfejlettebb államokban napjainkban már szinte „mobil laboratóriumok" vannak a helyszíni szemléken. Ezeket a mély fizikai-biológiai-kémiai-(ballisztikai, genetikai-daktiloszkópiai) ismeretekre épülő minilaborokat csak azokhoz speciálisan kiképzett személyek, szakértők kezelhetik és szerezhetnek velük megbízható adatokat.

[8] KATONA Géza megfogalmazásában: „A tudományos tanácskozások megerősítették azokat a nézeteket, amelyek szerint a kriminalisztikai szakértés a büntetőeljárásbeli felderítés és bizonyítás szerves része, egyben híd a tudományok és a bűnüldözés között." Illetve, hogy 2010-ben a magyar bűnügyi technikusok „83000 bűnügyi szemlén mintegy 510000 nyomot rögzítettek" KATONA Géza: A kriminalisztikai szakértés új szakasza a huszonegyedik század kezdeti éveiben. Belügyi Szemle, 2011/6. 18. o.

B) Ugyanakkor azt is láthatjuk napjaink bűnüldözésében, hogy nem csak az „első csapásos" szemlés ügyek – élet-testi épség elleni, nemi bűncselekmények, betörések, közlekedési és munkahelyi balesetek stb. – kívánják meg a szakértői bekapcsolódást.

Az ún. fehér galléros, gazdasági vagy cyberbűncselekmények is könyv-pénzügyi-bank-deviza-írás-cyberszakértőkért kiáltanak[9], az általános nyomozói kirminálmetodikai ismeretek már nem elégségesek. Fogynak azok az egyszerű ügyek – főleg a verbális módon elkövethetők maradnak –, amelyekben nincs szükség valamilyen különleges szakértelmet igénylő kérdés megválaszolására.

C) Lassan elfogynak azok a hagyományos kriminál taktikai cselekmények is, ahol nem hív a gyakorlat segítségül valamilyen szakértőt. Már a bizonyítási kísérleteknél, (ház-, gépjármű-kamionkutatásoknál, lefoglalásoknál is sokszor ott vannak, és ott kell lenniük). Gondoljunk csak a fegyvert, robbanószert kereső eseményekre vagy a számítógéppel – hardverrel, szoftverrel, nyomtatóval, szkennerrel, másolóval, faxkészülékkel – kapcsolatos elkövetésekre. Mindkét csoportnál minőségi specializációra van szükség, így a (digitális) nyomok-anyagmaradványok szakszerű felismerése, rögzítése, elszállítása körében, nem is beszélve a további vizsgálatukról, beltartalmuk, jellemzőik megismeréséről.

6. Valószínűségi szintemelkedések

A) Összhangban az eddig felsorolt tendenciákkal, nem meglepő, ha azt állítjuk, hogy a minőségi specializálódás, a mikro-nanoméretű szemlélődés és egyre fejlődő eszközű vizsgálat, amelynek egyre erősebb az élessége, azt az eredményt hozza a sokasodó és egyre szélesebb spektrumot felölelő szakértői vélemények körében, hogy a megállapítások, konklúziók is magasabb minőség felé haladnak tendenciózusan. Úgy is fogalmazhatunk, hogy folyamatos közeledés van az „1"-es érték, azaz a bizonyosság felé már egy-egy szakértői vélemény kapcsán is, nem csak a bizonyítékok összessége tükrében.[10] Ahogyan napról-napra élesebben és

[9] Tóth Mihály: Gazdasági bűnözés és bűncselekmények. KJK-KERSZÖV Kft. Budapest, 2002. 61-73. o.; valamint Herke Csongor: A műszaki és könyvszakértői vélemény egyes sajátosságai. In: Elek Balázs – Háger Tamás – Tóth Andrea Noémi (szerk.): Igazság, ideál és valóság: Tanulmányok Kardos Sándor 65. születésnapja tiszteletére. Debrecen, 2014. 196-209. o.

[10] Wolfgang Steinke megfogalmazása szerint is fontos kérdésről van szó, hiszen: „Az igazságügyi szakértői gyakorlat egyik legfontosabb kérdése a bűnügyi technikai szakvélemény bizonyító értéke, mert a jogalkalmazónak tudnia kell, hogy milyen valószínűséggel helyesek a szakértő megállapításai, egyáltalán mennyit ér a szakvélemény." Steinke, W.: A bűnügyi technikai szakvélemények bizonyító

mélyebben lát, ismer meg a tudományos eszköztár, úgy nő az esélye a valószínűségi arány növekedésének is. A modern kriminalisztika kezdetén, a XX. század elején például nem volt biztos az anyagmaradvány vér eredete. Miután – a kémiai-biológiai módszerek által – bizonyossá vált, jött annak kategorizálása, hogy kié a vér, a vércsoportok alapján. Napjainkban pedig az egyre bővülő alfaktorok tudása alapján már az a kérdés, hogy kié bizonyosan („1-es" értékkel) a vér.

B) A paradigma váltásként jelentkezett DNS azonosítás esetében is folyamatosan nő a megismerés, a tudás valószínűség szintje, ahogyan finomodik, cizellálódik a szakmabéli tudás, a vizsgálati metódus technikája, a végrehajtási eszközparkja és segédanyagai. Azt is tényként állítható, hogy egyre kisebb mintamennyiségre van szükség egyre magasabb szintű megismeréshez. Tendenciájában lehet számítani talán még arra is a jövőben, hogy a mikor keletkezett kérdésére is pontos választ kapunk, amikor egy anyagmaradványt vizsgálunk a DNS tükrén keresztül. Hasonló folyamat zajlik napjainkban a digitális adatok körében, amelyek mögött a tettes azonosítása még számtalan buktatót rejt magában, azonban a kriminál-technikai módszerek fejlesztésével párhuzamosan itt is valószínűség növekedést érzékelünk.[11]

C) A DNS minták bűnügyi elemzésében már bizonyítottan elfogadott, matematikára épülő Bayes-analízis segítséget nyújthat a szakvélemények valószínűségi szintjének értékelésében is. Ha a most is még megjelenő módszertani hibákra a kutatók felhívják a figyelmet és azokat az alkalmazók elkerülik, jó eséllyel számolhatunk a további értéknövekedésre. A bayesi megközelítés egyébként a kriminalisztikán túlmutató előnyökkel szolgálhat a büntetőeljárásban, a büntetés-végrehajtásban, a kriminológiai előrejelzésekben, a polgári perbeli bizonyításban és a bűnmegelőzés szélsőséges esetében, a terrorelhárításban is.[12]

értéke. In: Katona Géza (szerk.): A kriminalisztika aktuális kérdései. BM Kiadó, Budapest, 2001. 94. o.

[11] Casey, Eoghan: Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press, New York, 2000.

[12] Lásd erről részletesebben Orbán József tanulmányait, köztük a digitális adatokért kiemelten: A felderítés és a nyomozás támogatása bayesi módszerekkel. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Modernkori veszélyek rendészeti aspektusai. Pécsi Határőr Tudományos Közlemények, Pécs, 2015. 169-174. o., illetve: A Bayes-hálók bűnügyekben. In: Finszter Géza – Sabjanics István (szerk.): Biztonsági Kihívások a 21. században. Dialóg Campus Kiadó, Budapest, 2017. 799-808. o.

7. Csapatmunka dominancia

A) A sokarcú, szerteágazó és egyre kiterjedtebb szervezett bűnözéssel szemben még az egyes bűncselekmények szintjén sem veheti fel a versenyt egy-egy kriminalista. Miután elengedhetetlenül szükséges a csapat, éppen ezen okból nincs is igazán vagy alig akad egyéni siker már napjainkban. A „team", a csapat, amely ma eredményeket produkálhat. Olyannyira csapat, hogy az már nem állhat meg – nemhogy az épületen belül – hanem az országhatárnál sem. Számtalan esetben nemzetközi (sokszor digitális) csapatmunkára,[13] összefogásra van szükség.

B) Kriminalisztikai alapelvnek tekintem „a minden kriminalista annyit ér, amennyi adata van" princípiumot. Ennek szellemében azt tudom mondani napjaink – és bátran állíthatom a jövő – tendenciájaként, hogy egy magányos, „szóló" kriminalista igen szűk és egyszerű ügycsoportban lehet csak sikeres. A kellő súllyal bíró, különösen szervezett jellegű, több szereplős ügyben folytatott „mononyomozás" nem bír átütő erővel. Oly sok adat – köztük az elektronikusok – van már a világ minden pontján, oly sok forrásból meríthet a kriminalista, hogy ezt megszerezni és áttekinteni egymagában nem tudja. Szüksége van segítőkre, társakra. Az egyes ügyekhez kapcsolódó sokféle verzióból eredő még több feladat sem engedi meg, hogy egy ember elvégezze és átlássa azokat. Ahogyan a szervezett bűnelkövetésben, úgy a szervezett bűnüldözésben is munkamegosztásra van szükség, és ez is jellemzi a XXI. század bűnüldözését. Azt is megkockáztatom, hogy visszavonhatatlanul.

8. Komputerizálódás („számítógépesedés")

A) A számítógép megjelenése és térhódítása kétirányú. Egyrészről megjelent és fokozottan megjelenik a bűnelkövetések körében mint elkövetési eszköz, illetve mint az elkövetés tárgya.[14] Számítógépekkel követnek el valóban „határtalan" csalásokat, terrorcselekményeket, személyiség lopásokat, illetve számítógépeket, programokat, csipeket „térítenek el" eredeti parancsaiktól, rendeltetésüktől. Továbbá a számítógép vált a fejlett országokban, és válik az egész világon az egyetlen íróeszközzé. Hiszen leesett a palettáról a múlt század „muzeális" jellegzetessége, az

[13] Joint Investigation Teams (JFT), – Nagy Judit erről és az összefogásról részletesen értekezik „Közös nyomozócsoportok az Európai Unió tagállamai közötti bűnügyi együttműködésben" c. PhD művében. Károli Gáspár Református Egyetem, Budapest, 2010.

[14] Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009.

írógép, és – úgy tűnik – lassan ez lesz a sorsa az író kéznek is. E század jellemzője a nyomtatott írás és az elektronikus írás. (Egyes USA államokban napjainkban már nem is kézírást, hanem számítógépes írást tanítanak az elemi iskolákban).

B) Másrészről a számítógép bűnüldözés-tudományi és felderítési eszköz. Ott található az alapkutatásokban, ám eszköz a kriminál technikai módszerek alkalmazásában is. (Például az AFIS, nyom- és anyagmaradványok azonosítása, személyazonosítás, hangazonosítás, FISH-Forensisches Identifizierungsystem Handschriften írásazonosítás körében.) Ugyanakkor a komputer adattároló-rendszerező és elemző is egyúttal, miután óriási kiterjedésű adathalmaz jön létre mind a hazai, mind a nemzetközi bűnüldözés révén.[15] Ezekből a minőségi, a releváns adat az értékes, vagyis a számítógépben levő adatot elemezni, szűrni, összefüggéseiben kell használhatóvá tenni (raszterezni). Itt is megjelenik egy paradoxon: a nagy általános, generális adathalmaz mögött az egyedi, speciális esetekben gyakran – minőségi – adatínség van.

C) Egyúttal itt is tendenciózusan folyik a nemzetköziesedés, a globalizált bűnüldözés, amelynek keretében folyamatosan kapcsolják össze az egyes nemzetek adatállományát. Ezt folyamatosan bővítik és intenzifikálják. Ennek konkrét megvalósulását láthatjuk például az Interpol, Europol,[16] Eurojust, Eurodac és Schengen keretében. A legutóbbi rendelkezik a nyomozást segítő ún. Schengeni Információs Rendszerrel (SIS I-II.), amely lehetővé teszi a keresett személyekkel, tárgyakkal (pl. gépjárművekkel) kapcsolatos adatok gyors cseréjét.

Az adatoknak összehasonlíthatóknak kell lenniük, ami a legkomolyabb problémát jelenti az eltérő jogi, statisztikai és informatikai alapú nemzetek között. Tekintve az egymástól nagymértékben különböző nemzeti büntetőjogi rendszereket, nem várható a közeljövőben átfogó egységesítés (homogenizáció), ugyanakkor az egyes bűncselekmények (tényállásaik) kapcsán – különösen, ami a szervezett bűnözést illeti –, már most is tapasztalható, és a jövőben nagy valószínűséggel még erősödni fog a törekvés egy legalább európai szintű egységesítésre.

D) A komputerizálódás tette és teszi lehetővé – az Amerikai Egyesült Államokból elterjedt – értékes, ún. bűnözési térképek (crime-mapping) készítését is, amelyet GIS (Geological Information System – német változatban: Geographisches

[15] Magyar részleteket közöl erről: Bozó Csaba – Déri Attila: A számítástechnikai alkalmazások térhódítása a bűnügyi technikában. Belügyi Szemle 2011/4. 98-128. o.

[16] Az Europolnak már van külön kiberbűnözés elleni központja is (European Cybercrime Centre, EC3). Lásd Mezei Kitti: Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. JURA 2018/1. 353. o.

Informationssystem) néven ismerhettünk meg.[17] Ez különböző adatbankokból származó információkat dolgoz fel és kapcsol össze egymással. Az eredmény egy optikai képes ábrázolás arról, mikor, hol és milyen típusú bűnözés lépett fel. Lehetővé teszi a „hot spot"-ok, a „forró helyek", vagyis a magas koncentrációjú bűnözéssel bíró, kis területi egységek azonosítását, az egyes megjelenési formák és hatásainak modellezését. A rendszer előnye, hogy nem utólag, „üldöző" módon, hanem szinte egy időben olvasható a bűnözési helyzetkép. Ennek alapján mind represszív, mind preventív intézkedések tehetők.

A bűnözési térképezés jövőbeni súlypontja a teljesen komputerizált, szinte önműködően lefuttatható adatelemzés, és az erre épülő automatikus előrejelzés a várható fejleményekre. A „hot spot" megfigyelt változásából például levezethető, hol és milyen valószínűséggel számíthatunk új „forró hely" felbukkanására. Állíthatjuk, hogy minél nagyobb teljesítményűek lesznek a számítógépek, annál hatékonyabban vethetők be a mesterséges intelligencia ezen rendszerei e területen is.

9. Kiberfelderítés („digitkommandó") előretörése

A) Az előző alpontban kiemelt számítógéppel van összefüggésben a cyber- vagy magyarosan kiberjelenség kiemelése, amely témánk szempontjából a dobogó tetején áll. Ám mint látható az eddigi rendszerezésből nem egyedül kapcsolódóik a digitális felderítéshez.

Az biztos, hogy nem lehet nem észrevenni a digitális adatok jelentőségének 2000-es évekbeli felerősödését. Ahogyan a cyberbűncselekmények[18] szaporodtak és szaporodnak, úgy szaporodtak és kell szaporodniuk a cyberfelderítési metódusoknak is.[19]

A kiberezés, a kibertér virtuális alapja az internet, amely egy 1983-as intézkedésnek köszönheti létét. Abban az évben ugyanis az addig szigorúan őrzött és

[17] Hartwig, M. A.: Geographische Informationssysteme. (GIS). Kriminalistik, 2001/5. 435. o.

[18] Moore, R.: Cybercrime. Investigating high-technology computer crime. Elsevier, Amsterdam-Boston-Heidelberg-London-New York-Oxford-Paris-San Diego-San Fransisco-Singapore-Sydney-Tokyo, 2010.; Higgins, G.: Cybercrime: An Introduction to an Emerging Phenomenon. McGraw-Hill, Boston, 2010.

[19] Valóságos cyberháború folyik. Lásd erről Nagy Zoltán András: A kiber-háború új dimenziói – a veszélyeztetett új állambiztonság. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" c. tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012. 221-233. o.

kizárólag hadászati célra használt kommunikációs rendszert leválasztották, és így született meg a polgári alkalmazhatósága. Ám ez még csak szakértelemmel használható fájlcserélésre és kommunikációra adott lehetőséget. A világhálót (World Wide Webet) 1991-ben adták a széleskörű felhasználók kezébe, akik közül a bűnelkövetők elég gyorsan felismerték a benne rejlő lehetőségeket. Ez a felismerés ma is tart és bővül folyamatosan. A világ 2013-as összlakosságának 7%-át kitevő használói körben a leggyakoribb visszaélések: tiltott pornográf felvételek készítése, tárolása, továbbítása[20], pedofília, zaklatás (cyberbullying), „üldözés" (stalking), személyazonosság ellopása, bankkártya-telefonkártya visszaélés, fémcsík kódlopás, csalás, pénzmosás, hamisított áruk és kábítószerek eladása, szerzői és szomszédos jogok megsértése[21], magánszemélyek-vállalatok-állami intézmények (pl. infrastrukturális) rendszere elleni („malweres" vagy túlterheléses) támadások[22], adathalászat (phishing), (informatikai) terrorizmus.[23]

B) Külön forenzikus mező jött létre az ilyen – transznacionális – jellegű bűncselekmények felderítésére,[24] és ez minden valószínűség szerint további, tendenciózus fejlődés előtt áll. Ez a terület pedig konkrétan a bűnügyi informatika („forensic computing" vagy „computer forensics",[25] „digital forensics", „cyber forensics"). Bármelyik kifejezést is nézzük, ugyanazon célról és feladatról szól: a számítástechnikai eszközök, rendszerek, vezeték nélküli hálózatok körében elkövetett bűncselekmények felderítésének elősegítése az ehhez szükséges digitális adatok felkutatásával, rögzítésével, vizsgálatával, értékelésével. (Joggal mondják, hogy „az adat az új olaj".)

Meglátásom szerint a második generációs bizonyítékok körébe tartozó digitális adatok elmúlt két évtizedes megjelenéséből és felértékelődéséből indul ki a tendencia. Ma már külön digitegységeket, „digitkommandókat" találhatunk a

[20] Lásd Dornfeld László – Mezei Kitti: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. Infokommunikáció és jog 2017/68.

[21] Nagy Zoltán András: A szerzői jogi jogsértések számítógépes környezetben, különös tekintettel a fájlcserére. Belügyi Szemle. 2004/11-12. 169-185. o.; Szathmáry Zoltán: A szerzői vagy szerzői joghoz kapcsolódó jogok megsértése nyomozásának jogalkalmazási anomáliái. Magyar Jog 2010/3. 153-157. o.

[22] Lásd erről: Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1. 66-83. o.

[23] Szabó Imre: Az informatikai terrorizmus veszélyei. Belügyi Szemle, 2011/2. 5-20. o., illetve Mezey Nándor Lajos: Kiberterrorizmus: valós veszély? Belügyi Szemle, 2011/2. 21-48. o.; valamint Nagy Zoltán András – Mezei Kitti: Az informatikai bűncselekmények. Egyetemi jegyzet, Pécs, 2017.

[24] Vacca, J.: Computer Forensics: Computer Crime Scene Investigation. Charles River Media, Hingham, MA, 2002.

[25] Kruse, W.-Heiser, J.: Computer Forensics: Incident Response Essentials. Addison-Wesley, New York, 2002.

legfejlettebb, leggazdagabb államok felderítői között, akik kellő, speciális szakértelemmel bírnak az ilyen jellegű bűncselekmények felderítéséhez, azon belül az ún. elektronikus helyszíni szemléhez, a speciális bűnjel „megőrzési lánc" fenntartáshoz, az online házkutatásokhoz. Nem lehet azonban pusztán a külön egységekre (kommandókra, unitokra) bízni az ez irányú bűnüldözést, hiszen ma már egyre több „szokásos", köznapi ismeretlen tetteses bűnügyben keletkeznek ilyen adatok. Gondoljunk csak a mobiltelefonok (cellapozíciók, SMS, MMS), házi számítógépek, bennük az e-mailes levelezések, (skype üzenetek, facebook lájkolások[26]) netbookok, laptopok, táblagépek adataira, amelyek relevánsak lehetnek a detektálás során.

C) A digitális – állandó és változó – adatok burjánzása, mennyiségileg óriási halmaza azonban nem feltétlenül záloga a sikeres digitnyomozásnak. Ugyanis számtalan akadály nehezíti a kriminalista dolgát. Nem kimerítő jelleggel felsorolok néhányat:
   a) az elkövető, illetve a konkrét számítógép használó személye mellett még az elkövetési hely is nehezen azonosítható, a hálózat jellege folytán ugyanis anonimitásba burkolóznak;
   b) ha netán sikerül azonosítani a számítógépes jelszót, azonosítót, lehet, hogy ezek álcázottak, mástól megszerzettek;
   c) a világ minden pontjáról – ezeket még váltogatva is – bűncselekményt lehet elkövetni, és még az is előfordulhat, hogy a kiinduló helyen nem is kriminális a cselekmény;
   d) a kibertéri adatok csak virtuálisan léteznek, a szó fizikai értelmében nyomot, anyagmaradványt nem találhat a kriminalista az adatok között bányászva, (ugyanakkor lehetséges találni a kiegészítő eszközökön, a hardver dobozán, vezetékeken, monitoron, klaviatúrán, egéren, kamerán, mikrofonon, hangszórón, lemezeken, pendrive-on stb.);
   e) alattomosan rejtve maradhatnak sokáig (vagy örökre) a tettek és következményeik, mivel a kvalifikált elkövetés és a sértetti kör átlagos vagy az alatti tudása, ismeretszintje, alkalmanként üzleti érdeke (pl. a bankoknál) nem teszi lehetővé a kellő idejű felismerést, illetve egyáltalán a feltárást.

D) A nehézségek áthidalására, az akadályok leküzdésére – pl. az adatok ki- és visszanyerésére – folyamatosan és tendenciózusan készülnek a világban a technikai-taktikai-metodikai-kriminálpolitikai ajánlások (monográfiák, tankönyvek,

[26] Önmagában a „lájkolásos-tetszikes" adatokból következtethetnek a kriminalisták a felhasználó nemére, etnikai hovatartozására, szexuális irányultságára, politikai beállítottságára, intelligenciájára, nyelvtudására, vallásosságára, utazásaira, esetleges jövedelmeire. A facebook üzenetekből, írásokból pedig szinte minden megtudható a magát kiadó, feltáró személyről.

jegyzetek, tanulmányok).[27] Konkrétan például a digitális adatokkal kapcsolatos bűncselekmények speciális helyszíni szemléjéhez, nyílt vagy titkos módszerű, eszközű felderítéséhez. Ezeknél a módszereknek széles tere van, hiszen éppen az egyik hatékony eszköz a használó tudta nélküli, „operatív", egyúttal virtuális beavatkozás, titkos adatbányászat, memóriamásolás.

10. Titkos eszközök és módszerek felértékelődése

A) Figyelemmel a világ bűnözésében az elmúlt évtizedekben bekövetkezett változásokra, gondolunk itt elsősorban a kábítószer-fegyver-prostitúció- műkincs-emberkereskedelmi, uzsora, szerencsejáték, védelmi pénzek szedése, terrorista[28] ügyekben tanúsított szervezettségre,[29] a globalizáció erőteljes növekedésére, biztonállíthatjuk, hogy a hagyományos, nyílt nyomozási módszerek nem elegendőek az eredményes bűnüldözés megvalósításához. Konspirált, széleskörű munkamegosztással, jelentős emberi és anyagi (szindikátusi) erőforrásokkal dolgozó hálózatokkal, személyekkel szemben csak titkos felderítési módszerekkel, kiterjedt spektrumú humán és technikai eszközökkel lehet hatékonyan fellépni. Ezt felismerték napjaink kriminalistái is, és szinte minden – fejlett, modern – állam bűnüldözési apparátusa él ezzel a lehetőséggel. Sőt a nagy horderejű, „fajsúlyos" ügyekben az eredményes felderítések mögött markánsan titkosszolgálati erők (informátor, bizalmi személy, titkos munkatárs, rezidens, az „F" objektum kezelője, a felderítő szervvel titkosan együttműködő más személy, kihelyezett munkatárs), eszközök (fedőokirat, mutatópénz, titkos együttműködési megállapodás, technikai adatgyűjtő eszközök, lehallgatások, hang-képrögzítések, speciális akció-gépjármű), módszerek (puhatolás, leplezett megtekintés és leplezett meghallgatás, megfigyelés, környezettanulmány, csapda, mintavásárlás, információvásárlás, operáció, játszma, akció, ürügy, legenda, dezinformálás, fedett nyomozó, bizalmi vásárlás, álvásárlás, ellenőrzött szállítás, bűnszervezetbe történő beépülés) rejtőznek.

[27] Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései. Magyar Jog, 2001/12. 726. o.; Mohácsi Barbara: Az online-házkutatás alkotmányosságának kérdései. In: A globalizáció kihívásai – kriminálpolitikai válaszok. Kriminológiai közlemények, Budapest, 2010. 201-210. o.

[28] Korinek László: A terrorizmus. In: Fenyvesi Csaba – Herke Csongor (szerk.): Emlékkönyv Vargha László egyetemi tanár születésének 90. évfordulójára. PTE ÁJK, Pécs, 2003. 169-181. o.

[29] Kőhalmi László: Die organisierte Kriminalität in Ungarn. In: Gál István László-Hornyák Szabolcs (szerk.): Tanulmányok Dr. Földvári József professzor 80. születésnapja tiszteletére. PTE ÁJK, Pécs, 2006. 165-182. o.

B) Az előző alpontban már részletezett digitális és ezen alpontban tárgyalt titkos eszközök tendenciájukban – az eredményes felderítéssel párhuzamosan – még egy jelenséget produkálnak. Nevezetesen, a „követhetőséget". Vagyis, hogy – az éppen a bűncselekményektől védendő – polgár folyamatosan „megfigyelés" alatt van,[30] virtuális és valóságos látókörben mozog. Ezerféle helyen veszik fel a köztéri-beltéri kamerák, mobiltelefonja állandóan adja a finom jeleket a pontos hollétéről, csakúgy mint a kocsijában levő GPS vagy jeladó készülék. Számítógépe – megcsapolható – e-mail üzenetei közvetítik gondolatait, bankkártyája – internetes vásárláskor – a személyes adatait. Ruházatát és testét a repülőtéren átvilágítják, és sorolhatnánk még tovább az eszközöket, helyzeteket, amelyek folyamatosan láthatóvá, felügyeltté és ellenőrzötté teszik a digitális dzsungelvilágban élő egyént.

11. Nemzetköziesedés (internacionalizálódás)

A) A XXI. században már nincs kétség afelől, hogy a bűnelkövetések régen átnyúltak az országhatárokon, de még a kontinenseken is. Globalizált a bűnözés is – pénzmosás,[31] szerencsejáték, kábítószerüzlet, embercsempészés, nukleáris anyagok illegális kereskedelme, prostitúció stb. – mint a profitszerzés egyik módja, miért lenne másként mint a gazdaság egészében. Ezzel szemben a bűnüldözésnek is globalizáltnak kell lennie, ha sikert kíván elérni. Szükség van tehát az államok, kontinensek, nemzetközösségek közötti együttműködésre és integrációra. Ismét egy „mögöttes-üldöző" cselekvési kikényszerítettségről van szó. Előbb volt a bűnözés határátlépése, mint a bűnüldözésé. Minden ország elemi érdeke a fokozottabb nemzetközi együttműködés, mind a bűnüldözésben, mind a bűnüldözés-tudományban. Az előbbi adatáramoltatást, kölcsönös informálást jelent, a másik a komplex felderítési-vizsgálati eljárások, metódusok egységes sztenderdjeinek kidolgozását. Ez csak az államok széles körére kiterjedő kooperációval és integrációval valósítható meg, amelyre vonatkozóan határozott a fejlődési trend. Gondoljunk itt a nap mint nap bővülő nemzetközi szintű intézmények felállítására, működtetésére, a tagállamok összefogására (Interpol, Europol, OLAF, Eurojust, Cepol, EASO, EIGE, FRA, Frontex).

[30] Korinek László megfogalmazása szerint: „Kezd kialakulni egy – ugyancsak a szorongásra visszavezethető – folyamat, a megóvottság egyúttal megfigyeltséget is jelent". Korinek László: Tendenciák. Belügyi Szemle, 2003/1. 57. o. Ugyanerről ír még: „Újabb tendenciák" c. tanulmányában is. Belügyi Szemle, 2013/1. 19-24. o.

[31] Gál István László: A pénzmosás és a terrorizmus finanszírozása az új magyar büntetőjogban. Belügyi Szemle, 2013/1. 26-56. o.

B) Mind az alapkutatások, mind az alkalmazotti technikák kipróbálásában, mind az egyes mintagyűjtemények – pl. fegyver, lőszer, cipőtalp, autógumi, gépkocsifesték, lakk, kézírás, gépírás, hang, dialektus, DNS – összekapcsolása folyamatban van, ezek nemzetközi egységben való koordinálása reális cél Európán belül és kívül is. Tendenciózusan élénkülnek az egyes szakterületek nemzetközi egyesülései is. Például ENFSI-FITEH – European Network of Forensic Science Institutes-Forenzikus Tudományokkal foglalkozó Intézetek Európai Hálózata; EDNAP – Európai DNS Laborok Egyesülete; European DNA Profiling Group – Európai DNS Profil Csoport; EAFS-EFTA – Európai Forenzikus Tudományok Nemzetközi Akadémiája.

Zárógondolat

A felsorolt, egymással kölcsönhatásban, laza vagy szoros kapcsolatban levő tendenciák világosan mutatják, hogy a XXI. század második évtizedének végén a modern bűnüldözés erősen támaszkodik a digitális adatok széles spektrumára. Nem túlzás azt sem állítani megítélésem szerint, hogy ezek felkutatása, összegyűjtése, megismerése és felhasználása nélkül korszerű, naprakész kriminalisztikáról nem is beszélhetünk. És meg merem kockáztatni azt a gondolatot is, hogy az elektronikus adatok (bizonyítékok) szerepe csak nőni fog a jövőben is.

Felhasznált Irodalom

Bozó Csaba – Déri Attila: A számítástechnikai alkalmazások térhódítása a bűnügyi technikában. Belügyi Szemle 2011/4.

Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press, New York, 2000.

Dornfeld László – Mezei Kitti: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. Infokommunikáció és jog 2017/68.

Fenyvesi Csaba: A kriminalisztika XXI. századi világtendenciái. Belügyi Szemle, 2013/10.

Fenyvesi Csaba: A XXI. századi bűnüldözés-tudomány nemzetközi tendenciái. Magyar Tudomány, 2004/6. 757-765. o.

Gaál Tibor: A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban. Belügyi Szemle 2018/7-8.

Gál István László: A pénzmosás és a terrorizmus finanszírozása az új magyar büntetőjogban. Belügyi Szemle, 2013/1.

HARTWIG, M. A.: Geographische Informationssysteme. (GIS). Kriminalistik, 2001/5.
HERKE Csongor: A műszaki és könyvszakértői vélemény egyes sajátosságai. In: Elek Balázs – Háger Tamás – Tóth Andrea Noémi (szerk.): Igazság, ideál és valóság: Tanulmányok Kardos Sándor 65. születésnapja tiszteletére. Debrecen, 2014.
HIGGINS, G.: Cybercrime: An Introduction to an Emerging Phenomenon. McGraw-Hill, Boston, 2010.
HORVÁTH Orsolya: Az emberi szag jövőbeni kutatásának lehetőségei és korlátai. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2013.
HORVÁTH Orsolya: Szolgálati kutyák a rendvédelemben: a múlt, a jelen és a jövő lehetőségei. Magyar Rendészet, 2015/3.
KATONA Géza: A kriminalisztikai szakértés új szakasza a huszonegyedik század kezdeti éveiben. Belügyi Szemle, 2011/6.
KORAJLIC, N., – TEOFILOVIC, N. – KESETOVIC, Z.: Terrorist act as crisis situation – challenge for investigators. In: NBP Journal of Criminalistics and Law. Kriminalisticko-Policijska Akademia, Beograd, 2009.
KORINEK László: A terrorizmus. In: Fenyvesi Csaba – Herke Csongor (szerk.): Emlékkönyv Vargha László egyetemi tanár születésének 90. évfordulójára. PTE ÁJK, Pécs, 2003.
KORINEK László: Tendenciák. Belügyi Szemle, 2003/1.
KORINEK László: Újabb tendenciák. Belügyi Szemle, 2013/1.
KŐHALMI László: Die organisierte Kriminalität in Ungarn. In: Gál István László-Hornyák Szabolcs (szerk.): Tanulmányok Dr. Földvári József professzor 80. születésnapja tiszteletére. PTE ÁJK, Pécs, 2006.
KRUSE, W.-HEISER, J.: Computer Forensics: Incident Response Essentials. Addison-Wesley, New York, 2002.
LACZI Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései. Magyar Jog, 2001/12.
MEZEI Kitti – TÓTH Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós – Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017.
MEZEI Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1.
MEZEI Kitti: Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. JURA 2018/1.
MEZEY Nándor Lajos: Kiberterrorizmus: valós veszély? Belügyi Szemle, 2011/2.

MOHÁCSI Barbara: Az online-házkutatás alkotmányosságának kérdései. In: A globalizáció kihívásai – kriminálpolitikai válaszok. Kriminológiai közlemények, Budapest, 2010.

MOORE, R.: Cybercrime. Investigating high-technology computer crime. Elsevier, Amsterdam-Boston-Heidelberg-London-New York-Oxford-Paris-San Diego-San Fransisco-Singapore-Sydney-Tokyo, 2010.

NAGY Judit: „Közös nyomozócsoportok az Európai Unió tagállamai közötti bűnügyi együttműködésben" c. PhD művében. Károli Gáspár Református Egyetem, Budapest, 2010.

NAGY Zoltán András – MEZEI Kitti: Az informatikai bűncselekmények. Egyetemi jegyzet, Pécs, 2017.

NAGY Zoltán András: A kiber-háború új dimenziói – a veszélyeztetett új állambiztonság. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" c. tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012.

NAGY Zoltán András: A szerzői jogi jogsértések számítógépes környezetben, különös tekintettel a fájlcserére. Belügyi Szemle. 2004/11-12.

NAGY Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009.

ORBÁN József: A Bayes-hálók bűnügyekben. In: Finszter Géza – Sabjanics István (szerk.): Biztonsági Kihívások a 21. században. Dialóg Campus Kiadó, Budapest, 2017.

ORBÁN József: A felderítés és a nyomozás támogatása bayesi módszerekkel. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Modernkori veszélyek rendészeti aspektusai. Pécsi Határőr Tudományos Közlemények, Pécs, 2015.

STEINKE, W.: A bűnügyi technikai szakvélemények bizonyító értéke. In: Katona Géza (szerk.): A kriminalisztika aktuális kérdései. BM Kiadó, Budapest, 2001.

SZABÓ Imre: Az informatikai terrorizmus veszélyei. Belügyi Szemle, 2011/2.

SZATHMÁRY Zoltán: A szerzői vagy szerzői joghoz kapcsolódó jogok megsértése nyomozásának jogalkalmazási anomáliái. Magyar Jog 2010/3.

TÓTH Mihály: Gazdasági bűnözés és bűncselekmények. KJK-KERSZÖV Kft. Budapest, 2002.

TREMMEL Flórián – FENYVESI Csaba – HERKE Csongor: Kriminalisztika. Dialóg Campus Kiadó, Budapest-Pécs, 2005.

TREMMEL Flórián: Magyar büntetőeljárás. Dialóg Campus Kiadó, Budapest-Pécs, 2001.

VACCA, J.: Computer Forensics: Computer Crime Scene Investigation. Charles River Media, Hingham, MA, 2002.

GYARAKI RÉKA

A KIBERBŰNCSELEKMÉNYEK MEGJELENÉSE ÉS HELYZETE NAPJAINKBAN

– Különös tekintettel a szervezett bűnözéssel kapcsolatos kérdésekre

Bevezetés

A szervezett bűnözés fejlődéséhez a kibertér és a különböző informatikai eszközök kiváló lehetőséget kínálnak, mert ezek segítségével a szervezett bűnözői csoportok nemcsak az egymás közötti kommunikációt képesek egyszerűbben megoldani, hanem a névtelenségük megőrzését is könnyebben tudják biztosítani. A következőkben a szervezett bűnözés és a kiberbűncselekmények közös kapcsolódási pontjait vizsgálom, kiemelt figyelmet fordítva a kibertérben elkövetett bűncselekményekre.

1. A szervezett bűnözés fogalma

A szervezett bűnözés általános fogalma alatt értjük többek között a következőket: a szervezett bűnözői csoport működésében résztvevő személyek profit elérésre törekednek, magas fokú szervezettség jellemzi, az elkövetők legtöbbször magasan képzett szakembereket vesznek igénybe az elkövetéskor, a szervezeten belül a munkavégzés tekintetében a centralizáltság jellemző és a szervezett tagjai sok esetben nem vagy csak a szükséges mértékben ismerik egymást. A szervezett bűnözők a céljaik elérése és a jogellenes cselekményeik elérése érdekében nem riadnak vissza a zsarolástól, a fenyegetéstől, a korrupciótól és a testi sértéstől vagy sok esetben az emberöléstől.

A szervezetten elkövetett bűncselekményeket a mély konspiráció, a tervezés, az időben elhúzódó végrehajtás jellemez. A szervezett bűnözés legfontosabb ismérvei a következők: monopolhelyzet létrehozása, extraprofit elérésére törekvés, a legális gazdasági struktúrák működtetése, valamint hierarchikus felépítés[1].

[1] Nyeste Péter: A nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú stratégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépés területén. Felderítő szemle XII. évfolyam 1. szám 2013. 111. o.

A szervezett bűnözéssel szorosan összefüggnek a gazdasági és az egyéb gazdasági jellegű bűncselekmények, mivel az illegális tevékenységből származó jövedelmet valamilyen legális, pénzmozgást feltételező (például alapítványi vagy gazdasági társaságok) mögé rejtve, tisztára mosva, próbálják meg leplezni. Ezáltal biztosítva, hogy a hatóságok ne észleljék, vagy ne találják meg a bűnös eredetű bevételeket. A pénzmosás esetében szükséges, tehát egy „pénz mosoda" létrehozása, amelynek felderítése és illegális tevékenységének bizonyítása a hatóságokat kihívások elé állítja.

A fogalom szükséges és gyakori elemei mellett megjelennek esetleges jellemzők is, mint a paramilitaritás (katonai jellegű), erős függőségi rendszer, amelynél előfordulhat politikai vagy ideológiai indíttatás, az elkövetéshez kapcsolódó holdudvar megjelenése.

A szervezett bűnözést a 2012. évi C. törvény a Büntető Törvénykönyv (a továbbiakban: Btk.) bűnszervezetként határozza meg, és aszerint olyan, a három vagy több személyből álló, hosszabb időre szervezett, összehangoltan működő csoport, amelynek célja az öt évi vagy ezt meghaladó szabadságvesztessel bűntetendő szándékos bűncselekmények elkövetése.[2] Ugyanakkor a jogszabály nem áll meg ennél a fogalomnál, hiszen szabályozza még a bűnszövetséget és a csoportos elkövetést is mint többes elkövetési formát.

Érdemes megemlíteni még, hogy önálló deliktumként került értékelésre a bűnszervezetben részvétel (Btk. 321. §), mely szerint, aki bűncselekmény bűnszervezetben történő elkövetésére felhív, ajánlkozik, vállalkozik, a közös elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyít feltételeket biztosítja, illetve a bűnszervezet tevékenységét egyéb módon támogatja, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel bűntetendő.

Jelen írásban felvázolt fogalmak és a tényállás részletes elemzésétől eltekintek, mert ezekkel egy másik fejezet foglalkozik részletesen.[3]

A fentiek fényében azt gondolom, hogy nem túlzás azt állítani, hogy azokat a sztereotípiákat már átléphetjük, hogy a szervezett bűnözés tipikusan csak a fegyver- vagy kábítószerkereskedelemmel, prostitúcióval vagy a migrációval[4] összefüggő deliktumokkal azonosítható, hiszen a technika fejlődését és a virtuális tér előnyös

[2] 2012. évi C. törvény 459.§ (1) bekezdés

[3] Lásd bővebben: Tóth Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009.; Nyitrai Endre: A szervezett bűnözés elleni küzdelem büntetőjogi és kriminalisztikai eszközei. PhD értekezés. Pécs, 2017. 23-41. o.; valamint Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017. 410-425. o.; Tóth Mihály – Kőhalmi László: A szervezett bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016. 603-626. o.

[4] Lásd bővebben: Hautzinger Zoltán: Idegen a büntetőjogban. AndAnn, Pécs, 2016.

oldalát a bűnelkövetők is maximálisan kihasználják, így már nemcsak mint elkövetési „eszközt", hanem az elkövetés helyeként és módszereként is a digitális világot választják.

Az informatikai rendszerek már lehetővé tették a XXI. században, hogy a különböző bűnszervezetek összekapcsolódjanak és kommunikáljanak úgy, hogy az anonimitásukat megőrizzék egymás előtt, az elkövetés gyorsabban és sok esetben precízebben történjen meg.

Jelen írásban a következőkre helyezem a hangsúlyt:

– Milyen bűncselekményeket követnek el meg a kibertérben a szervezett bűnözés körében?
– Milyen előnyeit használják ki az egyes szervezett bűnözői körök az információs rendszereknek és eszközöknek?
– Mire irányulhat a bűnszervezeteknek a figyelme a virtuális tér által kínált lehetőségeknél?
– Milyen kihívásokkal kell szembenéznie a hatóságoknak a fentiek fényében a bűncselekmények felderítésénél?

1.1. A modernkori szervezett bűnözés

A szervezett bűnözésről még mindig sok embernek az olasz maffia vagy éppen a dél-amerikai drogkereskedők jutnak az eszükben, így akár Al-Capone vagy Pablo Escobar.

A szervezett bűnözésnél jellemző a folyamatos megújulás, a kockázatvállalásnak a legminimálisabb szintre történő csökkentése, amelyek akár a szigorú életviteli, viselkedési szabályok megalkotását, betartását kívánják meg.

A szervezett bűnözői csoportok megváltoztak, sok esetben nem is ismerik már egymást személyesen, és egyre inkább az általuk elkövetett hagyományos, fizikai világhoz kapcsolható deliktumokat felváltja a kibertérben vagy az informatikai eszközök felhasználásával elkövetett bűncselekmények köre. A technika segítségével már az sem szükséges, hogy földrajzilag egy helyen legyenek, találkozzanak, egymásról a nick nevükön – esetleg e-mail címükön – kívül bármit is tudjanak. Sőt minél kevesebbet tudnak a bűnszervezet tagjai egymásról, annál nagyobb az esély, hogy a nyomozó hatóságok előtt nem lesznek mindannyian ismertek, ezáltal a felderítés ellehetetlenül vagy nehézkessé válik.

1.2. SOCTA

Először is szükséges beszélni az Európai Multidiszciplináris Platformról (European Multidisciplinary Platform against Criminal Threats – EMPACT), mely programot a bűnügyi fenyegetések elleni fellépések érdekében hoztak létre.

Az EMPACT Program az Európai Unió hatálya alatt, a nemzetközi szervezett bűnözés elleni hatékony fellépés sürgetése érdekében létrehozott olyan feladatrendszer, amelynek keretében számos eltérő prioritáshoz (így például a kiberbűncselekmények, az emberkereskedelem, a kábítószerkereskedelem és előállítás stb.) kapcsolódóan közös munkát végeznek az erre kijelölt EMPACT nemzeti szakértők az Europol-lal együtt.

A számítógépes bűnözés[5], valamint az internetes bűnözés elleni harc prioritást élvez, és ezeken belül kiemelten a bankkártya bűnözéssel, a kibertámadásokkal és gyermekek online szexuális kizsákmányolással szemben van szükség a közös fellépésre.

E szakterületet uniós szinten az Europol képviseli, melynek egyik fontos feladata, hogy elemezze és értékelje az Európai Uniót érő súlyos és szervezett bűnözési fenyegetettségét, melyről jelentést készít évente (Serious and Organized Threat Assessment – SOCTA).

A SOCTA jelentés készítésének célja a bűnelemzés (crime intelligence analysis), továbbá a bűnügyi és más, bűnügyileg érdemleges információk közötti összefüggés felismerése, azonosítása és azok értékelése, mely elősegítheti a rendszeres, célirányos és összehangolt tevékenységet.

A jelentés foglalkozik a tagállamonként azonosított bűnszervezetek számával, jellemző tevékenységi területeikkel, az általános bűnügyi helyzetre vonatkozó adatokkal, ami egyben a statisztikai szemlélet erősödésére utal. Világosan megfogalmazza a bűnszervezetek, illetve a súlyos és szervezett bűnözés képviselte fenyegetettség jellegét és a fellépés érdekében szükséges prioritásokat, melyek szakpolitikai elfogadása (legalizálása) is megtörtént.[6]

Az Európai Unió Tanácsa 2010-ben elfogadta az EU szakpolitikai ciklusát, amelyben a 2014-2017-es ciklus egy „árucikk" szerű megközelítést tartalmaz. Ebben a ciklusban 9 prioritási területre bővült a bűncselekmények kategória szerinti osztályozása a Tanács 8453/2/2013-es dokumentuma alapján:

[5] Bővebben erről: Parti Katalin – Kiss Anna: A számítástechnikai bűnözésről akkor és most. In: Bárd Petra – Hack Péter – Holé Katalin: Pusztai László emlékére. OKRI-ELTE ÁJK. Budapest, 2014. 297-310. o.

[6] A speciális felkészültséget igénylő elemzés kialakulása egy új rendvédelmi szakterületnek a létrejöttét eredményezte: a bűnelemzését. A taktikai és stratégiai bűnelemzés gyakorlata szakértői tevékenységként az 1970-es években jelent meg az Interpol révén. E szervezet közvetítésével az 1980-as években a magyar kriminalisztika részéve is vált a bűnelemzés. Lásd Urszán József: A szervezett bűnözés fenyegetettség értékelésének jelentősége az Európai Unióban. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Pécsi Tudományos Határőr Közlemények. Pécs, 2013. 434-435. o.

1. Az illegális migráció elősegítésének a megakadályozása, különös tekintettel az uniós országok belépési pontjain, a főútvonalakon, valamint a forrás országokban,
2. a munkaerő szexuális célú emberkereskedelem visszaszorítása a legjelentősebb forrás országokból,
3. az egészségre, a biztonságra, az élelmiszerbiztonságra vonatkozó hamis termékek gyártásának és kereskedelmének megakadályozása,
4. jövedéki csalás és az MTIC281 („Eltűnő kereskedő a közösségen belül" jellegű csalás),
5. a kábítószerkereskedelem csökkentése,
6. a pénzügyi szolgáltatók elleni csalások csökkentése,
7. a számítógépes bűnözés visszaszorítása, elsősorban a bankkártya-csalás, a gyermekek online szexuális kereskedelme, valamint az infrastruktúrát és az informatikai hálózatot érő kibertámadások területén,
8. az illegális fegyverkereskedelem,
9. a bevándorló bűnözői csoportok által elkövetett tulajdon elleni bűncselekményekkel szembeni fellépés.

Az Európa Tanács Szervezett Bűnözés Büntetőjogi és Kriminológiai Kérdéseivel Foglalkozó Szakértői Csoportja (PC–S–CO) megfogalmazta azokat a követelményeket, amelyek fennállása esetén megállapítást nyerhet a bűnszervezet léte.

A Szakértői csoport által kötelező kritériumok szükségesek:

a) három vagy több személy együttműködése;
b) hosszú távú vagy határozatlan időre szóló együttműködés;
c) súlyos bűncselekmények gyanúja vagy azok elkövetése;
d) anyagi haszonszerzési és/vagy hatalmi pozícióba kerülési cél.

Az esetleges kritériumok:

a) minden egyes résztvevőnek meghatározott feladata vagy szerepe van;
b) valamely belső fegyelmi vagy ellenőrzési forma használata;
c) megfélemlítés céljából erőszak vagy egyéb eszközök alkalmazása;
d) befolyás kiterjesztése a politikusokra, a médiára, a közigazgatásra, a rendészeti szervekre, az igazságszolgáltatásra, illetve a gazdasági élet szereplőire a korrupció vagy bármely más üzleti módszer alkalmazásával;
e) kereskedelmi vagy üzleti jellegű struktúrák alkalmazása;
f) részvétel a pénzmosásban;
g) nemzetközi szintű működés.

Ahhoz, hogy a csoport bűnszervezetnek minősüljön a szakértői csoport szerint a kötelező kritériumoknak együttesen és legalább kettő esetlegesnek kell megvalósulnia.[7]

A szervezett bűnözői csoportok beazonosításához egyaránt nemzetbiztonsági és rendőrségi tevékenységre szükség van, azonban a bomlasztásuk és felszámolásuk már kizárólag rendőrségi feladat.[8]

A 2000-ben elfogadott Palermói egyezmény[9], amelyet az Egyesült Nemzetek Szervezete épp a szervezett bűnözésben, a szervezett bűnözői csoportok felszámolásában, az ilyen jellegű bűncselekmények észlelése kapcsán fogadott el az ahhoz csatlakozó államok feladatainak meghatározása céljából.

Az Egyezményben a részes államok többek között vállalják a korrupcióval és a pénzmosással összefüggő cselekmények bűncselekménnyé nyilvánítását, valamint a részes államok hatóságai közötti – így a nyomozó hatóság, ügyészség, valamint a hatóságok és pénzintézetek közötti effajta bűncselekményekre vonatkozó együttműködést, egymás felé küldött jelzéseket, az elemző értékelő munka végrehajtásának és eredményeinek egymás közötti megosztását.

Amennyiben az Egyezmény elfogadásának időpontját megnézzük, úgy érthető, hogy a szervezett bűnözést és a kiberbűncselekményeket még összefüggésében nem említi, ugyanakkor a következőkben érthető lesz, hogy ez a hiányosság nem jelenti azt, hogy ez a két fogalom nincs összefüggésben egymással.

2. Szervezetten elkövetett bűncselekmények a kibertérben

A kiberbűncselekmény általános fogalma alatt az informatikai eszközök és/vagy rendszerek segítségével, vagy az informatikai eszközök és hálózatok ellen elkövetett bűncselekmények értendők, amelyek céljai lehetnek a rendszerben tárolt adatok megszerzése, a jogosultak számára hozzáférhetetlenné tétele, továbbá az elektronikus rendszerbe vetett bizalommal visszaélés.[10] A kiberbűncselekmények további

[7] KIRIPOVSZKY Csaba: Az emberkereskedelem és a szervezett bűnözés kapcsolata a prostitúció tükrében. Pécsi Határőr Tudományos Közlemények VIII. Különszám. Pécs, 2007. 79–80. o

[8] NYESTE: i.m. 111. o.

[9] Magyarországon az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény kihirdetéséről szóló 2006. évi CI. törvénnyel került bevezetésre.

[10] SZATHMÁRY Zoltán a következőképpen határozza meg a számítástechnikai bűncselekmény fogalmát: „az a bűncselekmény, mely a számítástechnikai rendszerek zavartalan működését, a bennük ke-

célja lehet az anyagi haszonszerzés[11], vagy az elektronikusan tárolt adatok illetéktelen felhasználása, vagy az azzal történő visszaélés.

Ezen típusú bűncselekmény elkövetési helye maga a kibertér[12] vagy, bár a virtuális térhez kapcsolódik az elkövetés – de leginkább az elektronikus információs rendszer felhasználásán van a hangsúly, de a fizikai térben történik maga a bűncselekmény.

Amikor kizárólag a virtuális térben történik az elkövetés, mint az információs rendszerbe történő jogosulatlan behatolás, kifürkészés esetén, az elkövető személyének megállapítása nehezebb vagy sokszor lehetetlen, hiszen a hatóságoknak és az érintett szervezeteknek elsődleges feladata – a tudomásra jutást követően – az okozott károk csökkentése és elhárítása, azonban a nyomozást és a felderítést nehezíti – sőt ellehetetlenítheti – az anonimitás és magasfokú látencia.

Azokban az esetekben, amikor az elkövetők leginkább az információs rendszert az elkövetés eszközeként használják – mint például a hirdetéses csalásoknál, zaklatásnál, gyermekpornográfiánál – akkor a szervezett bűnözői körök sokkal több nyomot hagynak maguk után, így a hatóságok megfelelő felkészülése, tudatossága esetén az elkövető megismerése és felderítése is eredményesebb lesz.

A következő bűncselekmények tekintetében jellemző a szervezett bűnelkövetés a kibertérben[13]:

- Pénzmosás (Btk. 399.§) megvalósulásának esetei online környezetben.
- Tiltott szerek forgalmazása, azzal való kereskedés:
- Kábítószer-kereskedelem (Btk. 176.§).
- Kábítószer készítésének elősegítése (Btk. 182.§).
- Kábítószer-prekurzorral visszaélés (Btk. 183.§).
- Új pszichoaktív anyaggal visszaélés (Btk. 184.§).
- Teljesítményfokozó szerrel visszaélés (Btk. 185.§).
- Egészségügyi termék hamisítása (Btk. 186.§).
- Piramisjáték szervezése (Btk. 412.§)

zelt adatok megbízhatóságához, hitelességéhez, titokban maradásához, illetőleg az ezekhez fűződő egyéb (nemzetbiztonsági, államigazgatási, gazdasági vagy személyes érdeket) sért, vagy veszélyeztet." Szathmáry Zoltán: A számítástechnikai bűncselekmények. Magyar Jog 2011/3. 162-163. o.

[11] Nagy Zoltán András: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1992/1. 26. o.

[12] A kibertér szabályozásával kapcsolatos kérdéseket lásd bővebben Dornfeld László: A kibertér főbb nemzetközi és nemzeti szabályozásai. In: Pintér István (szerk.): Műhelymunkák: A virtuális tér geopolitikája. 43-88. o.

[13] Nagy Zoltán András NKE RTK Kiberbűnözés Elleni Tanszékének vezetője által felsorolt kibertérben elkövethető bűncselekmények

– Rossz minőségű termék forgalomba hozatala (Btk. 415.§)
– Fogyasztók megtévesztése (Btk. 417.§)
– Tiltott szerencsejáték szervezése (Btk. 360.§) és más bűncselekmények.
– Támadások kormányzati szerverek ellen.
– Támadások kritikus infrastruktúrák ellen.
– Támadások a pénzügyi szféra ellen (pl. DDoS-támadások, ransomwareek, APT támadások, MITM-, WITM-támadások, booster/streamer visszaélések stb.)
– Készpénz-helyettesítő fizetési eszközök elleni támadások:
– Készpénz-helyettesítő fizetési eszköz hamisítása (Btk. 392.§).
– Készpénz-helyettesítő fizetési eszközzel visszaélés (Btk. 393.§).
– Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése (Btk. 394.§)

2.1. A szervezett bűnözés és a kiberbűncselekmények

A szervezett bűncselekmények és a kibertérben elkövetett bűncselekmények kapcsolódási pontjait a következő szempontok alapján csoportosítottam:

– Kibertérben elkövetett olyan bűncselekmények, amelyeknek a tárgya az információs rendszer;
– Az informatikai eszközök felhasználásával elkövetett bűncselekmények;
– Az informatikai eszközök mint kommunikációs eszközök.

A kibertér kifejezést szükségesnek éreztem kihangsúlyozni, hiszen, ahogy fentebb is említettem, amennyiben maga a számítógép mint tárgy ellen követnek el fizikai támadást, így lopást, rongálást, az még önmagában nem kiberbűncselekmény. Amennyiben maga az információs rendszer ellen, vagy az abban tárolt adattal összefüggésben követnek el bűncselekményt, akkor az már kiberbűncselekménynek (kibertámadásnak) minősül. Ilyen támadási formák az információs rendszer megsértése – vagyis meghekkelése, a rendszer ellen irányuló, zsarolóvírusok, malware-ek, a túlterheléses támadások (DDoS támadás)[14], vagy egy honlap megrongálása (defacement) is.

A felsorolt támadások hátterében a károkozás, a megfélemlítés, a zsarolás és mindennek előtt a pénzszerzés áll.

[14] Lásd erről: Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1. 66-83. o.

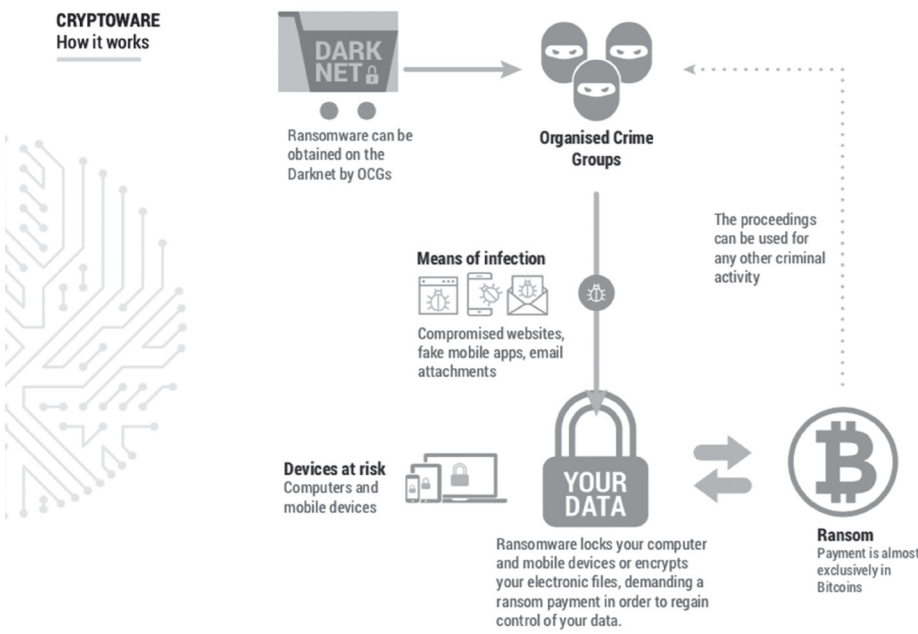
2.2. A szervezett bűnözés megjelenése és ismérvei a kibertérben

A bűnszervezetek egyre szélesebb körben használják ki az internet és az informatikai eszközök nyújtotta lehetőségeket a különféle jogellenes cselekményeik elrejtésére.

A szervezett bűnözői csoportok által elkövetett bűncselekményeknek az egyik piactereként szolgál az ún. Darknet, amely egy speciális Tor Browser nevű böngészővel használható, amelynek egyik előnye, hogy a magas fokú anonimitása révén megnehezíti a felhasználók azonosítását.

A Darkneten, azaz az internet sötét oldalán, a bűnözők képesek rejtve maradni, ugyanakkor az illegális termékeket vagy szolgáltatásokat, mint egy piacon kínálni (pl. bérgyilkos szolgáltatását vehetik igénybe, fegyvereket vagy kábítószert szerezhetnek be).

A SOCTA 2017-es jelentése alapján, a 2017. januárig több, mint 1,7 millió közvetlen felhasználója volt a Tor hálózatnak.



1. ábra: Az ún. cryptoware működése[15]

[15] Forrás: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 [2018.05.02.]

2.2.1. Gyermekpornográfia

Az egyik legnagyobb problémát jelentő és egyben a bűnszervezetek számára a legnagyobb bevételt generáló bűncselekmény a gyermekpornográfia[16] (Btk. 204.§), amelyet az online térben történő elkövetés mellett a fizikai térben is megvalósuló gyermekek szexuális kizsákmányolása, vagy abúzusa jelenti.[17] Az elkövetők az internet lehetőségeit maximálisan kihasználva, osztják meg egymás között a 18. életévüket be nem töltött személyekről készült szexuális tartalmú vagy a szexuális vágy felkeltésére alkalmas olyan felvételeket, amelyek elérése – az adott oldalról a letöltése, hozzáférhetővé tétele – vagy pénzért, vagy hasonló felvételekért cserébe valósul meg. Az elkövetők legtöbbször az érdeklődési területükből kifolyólag magányosak, ugyanakkor az internetnek köszönhetően egymással kommunikálnak könnyedén, valamint az általuk elkövetett bűncselekményekből származó felvételeket egymással megosztják (pl. a szexuális kényszerítés, szexuális visszaélés vagy vérfertőzés révén a saját közvetlen családtag segítségével járulnak ehhez hozzá). Például ezeket a képeket, videókat saját zárt csoportjukban online, vagy ritkább esetben adathordozón továbbítják egymásnak, azaz a Btk. 204. §-ban meghatározott elkövetési magatartásban meghatározottak alapján felvételre veszik és megosztják.

A gyermekpornográfia bűncselekményével kapcsolatban a szervezett bűnözői körök nemcsak az ilyen beállítottságú emberek személyét ismerik meg, hanem azok személyes adatait (bankkártya adatait) is, amely által zsarolhatóvá válnak, vagy az adataikkal visszaéléseket, esetleg egyéb bűncselekményt követnek el, ezáltal az elkövetők sértettek is lesznek, amelyet ritkán hoznak a hatóság tudomására, félve a rájuk váró szankcióktól.[18]

2.2.2. Tiltott szerek forgalmazása

A felsorolt bűncselekményekkel kapcsolatban a tiltott szerek forgalmazása és az ezekkel való kereskedés a kibertérben történhet az online fekete piactereken, ahol leggyakrabban a kábítószerek, illetve egyéb tiltott szerek adásvétele zajlik. A Darkneten megvalósuló illegális üzleti tevékenység kifejezetten azoknál a szolgáltatásoknak és termékek értékesítésének nyújt kiváló teret, amelyekhez a törvény által tilalmazott magatartások kapcsolódnak.

[16] Lásd bővebben Parti Katalin: Gyermekpornográfia az interneten. Bíbor Kiadó. Budapest, 2009.

[17] Dornfeld László – Mezei Kitti: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. Infokommunikáció és jog 2017/68. 33. o.

[18] Mezei Kitti – Nagy Zoltán András: The organised criminal phenomenon on the Internet. Journal of Eastern-European Criminal Law 2016/2. 145. o.

Ugyanakkor nemcsak a rejtett piacterek használhatók e célból, hanem sok esetben akár a közösségi oldalakon vagy az egyszerű keresőmotor által elérhető weboldalakon is megtalálhatóak ezek a termékek – akár internetes hirdetésekben, ún. bannerekben elhelyezett reklámok révén –, és megvásárolhatóak (pl. azon gyógyszereket, amelyek hatóanyaguk révén akár kábítószernek, vagy illegális teljesítményfokozónak minősülnek és épp emiatt az adott országban legálisan nem kerülhet forgalomba).

Ugyanígy kedvez az internetes vásárlás a hamis vagy rossz minőségű gyógyászati termékek értékesítésének vagy a pszichoaktív anyagok készítésének (pl. az alkotóelemeinek, összetevőjének árusítása révén, az azzal történő kereskedéssel, valamint az elkészítéshez szükséges további instrukciók nyilvánossá tételének megosztásával).

2.2.3. Piramisjáték szervezése

A piramisjátékok szervezése virágkorát éli továbbra is napjainkban. A számítógépes technológia tömeges elterjedése előtt is már jelent volt e tradicionális deliktum[19], azonban új dimenzióba lépett az internet és a közösségi médiák térhódításával, mert a korábban ismerősök által történő beszervezés és hálózatépítés átalakult. Most már nem szükséges a bemutatókra és csapatépítésekre járni, de még az sem szükséges, hogy valaki a saját házába fogadja a látszólag MLM rendszert kínáló szervezőt. Elég, ha e-mailen vagy bármilyen más elektronikus eszközön – mobiltelefonon keresztül szóban megvalósuló egyetértő kifejezéssel – keresztül történő szerződéskötés, amely joghatás kiváltására alkalmas[20].

A piramisjáték szervezéséhez az internet és az általa kínált lehetőségek kifejezetten alkalmasak arra, hogy kevés szervezéssel, elegendő számítógép felhasználói ismerettel nagyobb tömeghez jusson el, mivel egy jól megtervezett honlap – ami lehet akár egy külföldi oldalnak a tükörmásolata – egy bankszámlaszám, egy létező vagy épp nem létező, de akár egy külföldön működő offshore cég létrehozásával tökéletesen kivitelezhető a piramisjáték. A szervezett bűnözői csoportok számára is kedvező a piramisjáték szervezése az online térben, hiszen az anonimitás biztosított – akár egymás előtt is –, az egymás közötti kapcsolattartásukat valamint a további tagok beszervezését egyszerűsíti, ráadásul egy jól megszerkesztett weboldalnak köszönhetően a bizalom elnyerése is egyszerűbbé vált minél több embernél. Mindez lehetővé teszi a számukra, hogy hosszabb időn keresztül folytassák a tevékenységüket, valamint, ha a nyomozóhatóságok eljárást indítanának, akkor azt követően

[19] Nagy Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! Magyar Jog 2016/1. 20-21. o.

[20] 2013. évi V. törvény a Polgári Törvénykönyv (Ptk.) 6:85.§ (1) bekezdés

más név alatt tovább folytathatják újabb áldozatokat gyűjtve. A játék szervezőjeként kizárólag a játék kitalálói, elindítói, fenntartói büntetendők. A beszervezett játékosok, akik a játék jellegéből fakadóan további játékosokat szerveznek be e bűncselekményben sem tettesnek, sem társtettesnek nem minősülnek.[21]

2.2.4. A rossz minőségű termék forgalomba hozatala

A rossz minőségű termék forgalomba hozatalának a fogyasztók érdekében végzett folyamatos ellenőrzések elkerülése miatt tökéletes színtere az internet. A Btk. értelmében rossz minőségű a termék, ha nem felel meg az EU ránk nézve közvetlenül kötelező jogi normában rögzített követelményeinek, valamint rendeltetésszerűen nem használható, vagy használhatósága jelentősen csökkent.[22]

A különböző aukciós és kirívóan olcsó termékeket árusító oldalakon, a közösségi oldalakon történő értékesítés esetén az eladó és a vevő közvetlenül lép úgy kapcsolatba – sokszor a külföldről történő rendelés esetén –, hogy azok a korábban Fogyasztóvédelmi Főfelügyelőségnek nevezett, mai elnevezése a Nemzeti Fogyasztóvédelmi Hatóság által végzett ellenőrzésekor – akár az elektronikus kereskedelmi tevékenység ellenőrzés során – sem juthat a rögtön a tudomására.

A leginkább az Európai Unión kívülről érkezett termékek esetében figyelhető meg – sokszor a jelentősen alacsonyabb árak miatt – hogy a magyar fogyasztók szívesebben rendelnek, még a hosszabb szállítási időbe is belenyugodva, a különböző kínai vagy ázsiai weboldalakról. Ezeken az oldalakon általában a következő – akár köztudottan hamis – termékeket rendelik: kozmetikai termékeket, ruhaneműket, ékszereket és játékokat, esetleg hamis csúcstechnológiai eszközöket. Ugyanez vonatkozik az adott országokon belül működő bűnszervezetekre, amelyek nemcsak, hogy rossz minőségű terméket „forgalmaznak", hanem a nagyobb bevétel érdekében még azokat silány minőségű anyagokkal keverik a nagyobb, de adózatlan bevételük érdekében.

2.2.5. Tiltott szerencsejáték szervezése

A virtuális hálózatokon is elterjedtek a különféle online szerencsejátékok.[23] Szerencsejátéknak minősül az 1991. évi XXXIV. törvény alapján[24] minden olyan játék,

[21] Molnár Gábor: Gazdasági bűncselekmények. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2009. 246. o.

[22] Tóth Mihály: XLII. fejezet – A fogyasztók érdekeit és a gazdasági verseny tisztaságát sértő bűncselekmények. In: Tóth Mihály – Nagy Zoltán: Magyar büntetőjog – Különös Rész. Osiris Kiadó. Budapest, 2014. 570. o.

[23] Nagy Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. Belügyi Szemle 2012/6. 114-115. o.

[24] 1991. évi XXXIV. törvény a szerencsejáték szervezéséről szóló törvény 1.§ (1) bekezdése

amelyben a játékos pénz fizetése, vagy vagyoni érték nyújtása fejében, meghatározott feltételek fennállása vagy bekövetkezése esetén pénznyereményre, vagy más vagyoni értékű nyereményre válik jogosulttá. A nyerés vagy a vesztés kizárólag, vagy túlnyomórészt a véletlentől függ.

Ahhoz, hogy legálisan lehessen szerencsejátékot szervezni a magyar törvények által előírt feltételeknek – így az adóhatóság felé történő bejelentési kötelezettség teljesítésével – meg kell felelniük, amelyeknek az ellenőrzése a hatóságok feladata. Ez az ellenőrzés – így a résztvevők életkora, a szervezők neve, a nyereményjátékban a nyeremény összegének kifizetése, egyáltalán a játék tisztasága a kibertérben nehezen vagy egyáltalán nem ellenőrizhető. A szervezett bűnöző csoportok felismerték és kihasználják ezt a lehetőséget, így a rendszerességet, a nagy nyilvánosságot megteremtve képesek a szerencsejáték lebonyolítására úgy, hogy abból adómentes bevételük származzon hosszabb időn keresztül. Amennyiben meg akarják teremteni a „tisztaság" látszatát, úgy a pénzmosást is megvalósítják tevékenységük során. Ennek egyik klasszikus formája lehet, amikor az internetes szerencsejáték során a szervezetthez tartozó személyek megvásárolják a játék részvétel jogát, majd attól elállva egy megadott – más személy – bankszámlaszámára utaltatják a pénzt, ahonnan aztán téves utalás címen visszakövetelik az összeget.

Arra is volt már példa, hogy az online pókerjáték során kártyázó hackereknek sikerült belenézni a játékosok lapjaiba. Ennek során a kiberbűnözőknek csak a trójai vírussal megfertőzött játékosokat kellett megtalálniuk[25], akiknek virtuális kártyalapjait módosították vagy épp a saját virtuális lapjaikat osztották, úgy hogy minél nagyobb összeget nyerjenek aztán a játékosoktól.

2.2.6. Készpénz-helyettesítő fizetési eszközökkel való visszaélések[26]

Az e-kereskedelem elterjedése, a különböző interneten keresztül történő fizetési lehetőségek (pl. szolgáltatók felé a közüzemi számlák kiegyenlítése, banki átutalások netbankon keresztül, PayPal vásárlás, bankkártyás vásárlások stb.) lehetővé tették, hogy a szervezett bűnözői körök a felhasználók bankszámlaszámát, a bankkártya adatait – sok esetben kérik a háromjegyű biztonsági kód megadását – megismerjék. Ez történhet akár egy trójai vírus segítségével, az eredeti honlap lemásolásával vagy

[25] ESET WeLiveSecurity blog

[26] Lásd bővebben a szabályozást: Mezei Kitti – Tóth Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós-Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017. 297-308. o

akár csalással (pl. telefonos csalás[27] vagy hamis banki e-mail elküldésével), majd az adatok felhasználásával, leemelhetik a bankszámlán lévő pénzösszeget, hamis bankkártyát készíthetnek vagy csekket állíthatnak ki maguknak.

Ugyanígy említést érdemelnek a kelet-európai vagy afrikai bűnözők által elkövetett ATM-en (Automated Teller Machine) vagy POS (Point of Sale-Terminals) terminálon keresztül történő bankkártya hamisítások is, amelyek esetében az áldozatok bankkártya adatait megszerzik, a számlájukon lévő pénzt a saját vagy más bankszámlájára utalják és azt később leemelik, vagy esetleg a hatóságok munkájának megnehezítése érdekében kriptovalutát, bitcoint vásárolnak belőle, amellyel aztán az arra alkalmas helyen felhasználnak, fizetnek vele.

Gyakoriak még az ATM-ek vírussal történő megfertőzése, amelynek során közvetlenül is hozzájuthatnak a számlán lévő pénzhez és adatokhoz. Ilyen esetben az elkövetők – vagyis, akik a vírusokat megírják –, nem feltétlenül lépnek ki a fizikai térben, hanem a káros programot a Darkneten vagy egy sima online piacon értékesítik, esetleg épp felkérésre írják meg, majd azt követően arra alkalmas személynek azt egy adathordozón, jellemzően pendrive-on átadják, annak leírásával együtt, hogy hogyan kell az ATM-et szétszedni és azon belül hol található annak behelyezésére alkalmas USB port, és milyen módon lehet a vírust telepíteni. Ezek a leírások általában egy átlag felhasználó számára érthetőek, nem igényelnek különösebb informatikai tudást.

Ebben az esetben a hatóság számára nehézséget okoz már annak a megállapítása, hogy ki az elkövető (az lesz-e, aki megírta a káros programot vagy az, aki telepítette azt a bankautomatára?), illetve mivel személyes kontaktus nem vagy csak nagyon ellenőrzött keretek között történik, a program írójának személye sokszor rejtve marad.

Az informatika fejlődését szervezett bűnözői körök is igyekeznek kihasználni, hiszen a kibertérben tudják legjobban az anonimitásukat megőrizni. Az internet határok nélkülisége, sok esetben szabályozatlansága vagy épp az országok eltérő jogi szabályozása az, ami leginkább segíti őket a céljaik elérésében.

2.2.7. Pénzmosás

A pénzmosás az előbbi alpontokban említett valamennyi bűncselekményekkel összefüggő olyan illegális tevékenység, amelynek célja, hogy a bűncselekményből származó anyagi nyereséget törvényes bevételnek tüntesse fel, olyan módon hogy az a hatóságok előtt rejtve maradjon, illetve az elkövetők kiléte ne legyen megállapítható.

[27] Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad librum, Budapest, 2009. 262. o.

A kiberbűncselekményekből származó bevételek elrejtésére az egyik legtökéltesebb eszköz, ha vagy egy legálisnak tűnő vállalkozást működtetnek, vagy pedig a megszerzett jövedelmet valamilyen kriptovalutába fektetik[28], amelynek ugyanakkor meg van a rizikója is, hiszen annak értéke folyamatosan változik és a felette való rendelkezés közel sem annyira egyszerű, mint a bankszámlán tartott pénzzé.

2.3. Támadások a kormányzati szerverek, a kritikus infrastruktúrák ellen

Érdemes azt is mérlegelni, hogy egy kibertámadás esetén mikor beszélünk a szervezett bűnözői körök által elkövetett bűncselekményről és milyen esetekben minősítjük a támadást terrorcselekménynek.

A kettő közötti különbség csekély. Talán az egyik legjellemzőbb eltérés a motiváció lehet, de ahogy Istanovszky László is rámutatott egy tanulmányában, az elkövetők célja a meghatározó.

Míg bűnszervezet esetében a cél az öt évi vagy azt meghaladó bűncselekmény elkövetése, addig a terrorista csoport[29] esetén a cél a terrorcselekmény elkövetése. A terrorcselekményekkel pedig a cél egy állam vagy szervezet kényszerítése, a társadalmi, gazdasági rend megzavarása, megrendítése, vagy a lakosság megfélemlítése[30].

Az Európa Tanács terrorizmus elleni küzdelméről szóló kerethatározatának[31] 2. cikk (1) bekezdése alapján: a „terrorista csoport" kettőnél több személyből álló, hosszabb idő alatt létrehozott, szervezett csoportot jelent, amely terrorista bűncselekmények elkövetése végett összehangoltan működik.

A „szervezett csoport" egy olyan csoportot jelent, amelyet nem egy deliktum azonnali elkövetésére hoztak létre alkalomszerű jelleggel, és amelyben a tagoknak nincs szükségképpen formálisan meghatározott szerepe, illetve nem szükséges a tagság folyamatossága vagy a fejlett struktúra.

A terrorista csoport és a bűnszervezet fogalmi elemei között több ismérv megegyezik, egyedül a célban mutatkozik különbség.[32] A szervezeti hasonlóság igazolható, amennyiben a Btk. bűnszervezetre és terrorszervezetre vonatkozó meghatározásait vetjük elemzés alá, az eltérés nem módszereikben, inkább céljaikban keresendő[33].

---

[28] Nagy Zoltán – Mezei Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog. 2018/70. 27. o.

[29] Btk. 319. § értelmező rendelkezés szerint a terrorista csoport: a három vagy több személyből álló, hosszabb időre szervezett, összehangoltan működő csoport, amelynek célja terrorcselekmény elkövetése.

[30] Istvanovszki László: A szervezett bűnözés elleni harc új stratégiája és taktikája. Hadtudomány Szemle 2015/1-2. 140. o.

[31] 2002/475/IB kerethatározat

[32] Lásd bővebben: Neparáczki Anna Viktória: A terrorizmus elleni fellépés eszközei a magyar és német büntető anyagi jogban. PhD értekezés. Pécs, 2017. 60-66. o.

[33] Istvanovszki: i.m. 139–143. o.

2.4. A szervezett bűnözők és a csúcstechnológiai eszközök fejlődése kínált lehetőségek

A szervezett bűnözők nemcsak a kiberteret használják ki, hanem a csúcstechnológia kínálta lehetőségeket is, amelyek révén akár írásban (titkosítva), akár szóban, a rendvédelmi szervek munkáját megnehezítve, képesek egymással kommunikálni, utasítást adni vagy sok esetben a helyszínt és a személyt feltérképezve segíteni egymás munkáját.

A modern eszközöknek köszönhetően más hálózatokhoz csatlakozva képesek rejtve maradni, de akár tőlük független személyek mögé bújva ismeretlennek lenni a hatóságok előtt.

A kommunikáció mellett a közösségi oldalak és a felhasználók kínálta lehetőségeket használják ki, amelyek során adatainkkal vagy a nem védett informatikai eszközeink felhasználásával követik el a bűncselekményt.

3. Nyomozási kihívások

A rendvédelmi hatóságok feladata[34] a bűnszervezetek működésének a felderítése[35], amelyet a kibertér használata és az országok különböző szabályozása vagy szabályozatlansága miatt igazi kihívást jelent.

A szervezett bűnözéssel kapcsolatban használt titkos hang-, beszéd-, kép-, videófelvételek a modern bűnüldözés nélkülözhetetlen eszközei, egyre inkább „conditio sine qua non”-jai az egyes nyomozásoknak, bizonyos bűncselekmények metodikájának.

A bűnelkövetők első dimenzióból második dimenzióba való átlépését követte a bűnüldözés hasonló irányú lépése is, amelyben felértékelődtek a második dimenziós bizonyítékok szerepe mint például az elektronikus bizonyítékoké. A hagyományos fizikai nyomokkal ellentétben már az az elektronikus nyomokat kell vizsgálni az információs rendszerek adattáraiban, adatok és adatmaradványok után kutatva, amelyekhez általában speciális tudású igazságügyi informatikai szakemberekre van szükség.[36]

---

[34] Lásd Simon Béla: A rendészeti szervek együttműködése a kiberbűnözés ellen. Nemzetbiztonsági Szemle 2018/1. 36-58. o.

[35] Ehhez lásd bővebben: Boda József: A felderítés, hírszerzés, titkos információgyűjtés elvei és gyakorlata. Belügyi Szemle 2015/9. 5-29. o.

[36] Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8. 441-442. o.; valamint lásd Máté István Zsolt: Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe. Belügyi Szemle 2018/7-8.

Az Európai Unióban az Europol-on belül a Számítástechnikai Bűnözés Elleni Európai Központ (EC3) foglalkozik a kibertérben elkövetett bűncselekményekkel, így kiemelten a szervezett bűnözői csoportok által elkövetett nemzetközi, online fizetési csalásokkal (az Európai Központi Bankkal és nemzeti bankokkal szoros együttműködésben), valamint a gyermekeket érintő szexuális kizsákmányoló magatartásokkal és a kritikus infrastruktúrákat érintő támadásokkal.[37]

Magyarországon a szervezett bűnözéssel valamint a kiberbűncselekményekkel kapcsolatban a Rendőrség és a Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatósága, a Terrorelhárítási Központ és az ügyészség foglalkozik, míg a nemzetbiztonsági szervezetek közül az Alkotmányvédelmi Hivatal, Katonai Nemzetbiztonsági Szolgálat feladatai között szerepel a szervezett bűnözők és a kiberbűnözők feltérképezése.

Ezen szervezeteken kívül ugyanakkor még meg kell említeni a Nemzetbiztonsági Szolgálat – Kibervédelmi Intézetet, a BM Országos Katasztrófavédelmi Főfelügyelőség, a Nemzeti Adatvédelmi és Információszabadság Hatóságot és a Nemzeti Média- és Hírközlési Hatóságot, amelyeknek kiemelt szerepe van a kibertámadások során.

Az Európai Unió 2014. június 10 és 13. között elfogadta a határokon átnyúló szervezett bűnözésről szóló Fehér Könyvet (Európa Tanács Büntetőjogi Kérdésekkel Foglalkozó Európai Bizottsága CDPC), amelyben kiemelték az Európai Unió tagállamait fenyegető veszélyeket, így a szervezett bűnözést, a kiberbűnözést valamint az Unió nyomozó hatóságainak és nemzetbiztonsági szervezeteinek ezzel kapcsolatos kihívásait.

A Fehér Könyv a következő példákon keresztül utal a nyomozási eljárások szabályozásának problémáira és ezzel összefüggésben a jogharmonizáció szükségességére:

– A számítógépek átkutatása gyakran a felkutatás és lefoglalás általános szabályai szerint történik, ami nem mindig jelent kielégítő megoldást, különösképpen problémás a számítógépes hálózatokhoz való távoli hozzáférés esetén. Az ilyenkor alkalmazott trójai és más hacker szoftverek használata határon túl joghatósági és szuverenitási kérdéseket vethet fel.
– Az adathalászat (phising) kapcsán bizonyos jogrendszerek nagyobb szabadságot biztosítanak a bűnüldöző hatóságoknak, úgy tekintve azt, mint a közterület-felügyeletet, ha az adat nyilvános forrásból származik, máshol viszont

36-54. o.; továbbá Herke Csongor: A műszaki és könyvszakértői vélemény egyes sajátosságai. In: Elek Balázs – Háger Tamás – Tóth Andrea Noémi (szerk.): Igazság, ideál és valóság: Tanulmányok Kardos Sándor 65. születésnapja tiszteletére. Debrecen, 2014. 196-209. o.; Simon Béla: Az igazságügyi szakértés egyes kérdései a büntetőeljárásban, különös tekintettel az informatikai szakterületre. Belügyi Szemle 2016/7-8. 87-105. o.

[37] Mezei Kitti: Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. JURA 2018/1. 353. o.

úgy vélik, az ilyen eljárások sértik a magántitokhoz való jogot, ezért alkalmazásukhoz meghatározott bírói ellenőrzés szükséges.
– Hasonló eltérések mutatkoznak az egyes tagállamoknak a szolgáltatást nyújtó vállalatok adatkezelési kötelezettségeire, illetve a nyomozó hatóságok ezen adatokhoz való hozzáférésére vonatkozó szabályozásaiban. Van, ahol bírósági végzés nélkül kiadhatók a felhasználók IP-címei, vagy akár az összes rájuk vonatkozó adat, máshol viszont csak a bíró hatalmazhatja fel a szolgáltatót, hogy a kliensek adatait a bűnüldöző szervek számára elérhetővé tegye.
– A határon átlépő ellenőrzött szállítások és a fedett nyomozók hatékony alkalmazását sokszor jogi akadályok és az egyértelmű szabályozások hiánya hiúsítja meg.
– Problémákat okoz, hogy több tagállamban nem határolódnak el egyértelműen a szervezett bűnözés súlyos formáinak felderítését végző titkosszolgálatok, információszerző egységek az állam védelmét ellátó nemzetbiztonsági szolgálatoktól.
– Nem egységes és sok helyen nem tisztázott, hogy milyen kényszerintézkedéseket foganatosíthatnak a hatóságok az eljárás egyes szakaszaiban[38].

A fenti problémák megoldása érdekében a dokumentum javaslatot tesz a tagállamok hatályos szabályozásának átfogó összehasonlító vizsgálatára és ennek nyomán egy kézikönyv, illetve egy folyamatosan frissülő weboldal létrehozására, valamint a különleges nyomozási eljárások transznacionális szinten való alkalmazásával, a bizonyítékok felhasználhatóságával és a terheltek jogainak védelmével kapcsolatos problémák további tanulmányozására. A munkacsoport szerint az Európa Tanácsnak kulcsszerepet kell játszania a határokon átnyúló büntetőeljárások általános elveinek kidolgozásában is.

4. Összegzés

Az említett bűncselekményekkel kapcsolatban felvetődik egy kérdés. Ezeket bűnszervezetek követik el, vagy pedig maga az elkövetés módja igényel szervezettséget? Nem technikai oldalról közelítve meg a felvetést, levezethetőek az alábbi megállapítások:

– A támadásokat rosszindulatú programok/szoftverek megírásával kezdik meg, aminek megírásához sok esetben nem elég egy személy, hanem több, egymást személyesen nem ismerő emberek követik el.

[38] http://www.juris.u-szeged.hu/kutatas-tudomany/tornyai-gergely/feher-konyv [2018.05.28.]

– Sokszor nem egy adott információs rendszer ellen hajtják végre, hanem eshetőlegesen, azok ellen, amelyek nem megfelelően (vagy egyáltalán nem) vannak védve, vagy esetleg egy úgynevezett backdoor-ral (hátsó kapuval) rendelkeznek és kihasználják annak gyengeségét
– A cselekmény végrehajtása a social engineering-gel vagy emberi manipulációval történik (ami szintén kérdéses kimenetelű és meg van a lehetősége, hogy egyáltalán nem vagy csak részben lehet kivitelezni).

Ezen a hármas tagolódást figyelembe véve, kiemelhető az elkövetők között a szerepek megosztása, ugyanakkor nem feltétlenül érvényesül a centralizáltság, hiszen a cél kivitelezéséhez technikailag legalább ugyanúgy kell érteni. A kivitelezés módjának informatikai, pszichológiai lehetőségeit és megoldásait sokkal egyszerűbb alakítani az elkövetők tudásához és habitusához, mint a hagyományosnak nevezhető szervezett bűnözőknél.

Felhasznált Irodalom

Boda József: A felderítés, hírszerzés, titkos információgyűjtés elvei és gyakorlata. Belügyi Szemle 2015/9.

Dornfeld László – Mezei Kitti: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. Infokommunikáció és jog 2017/68.

Dornfeld László: A kibertér főbb nemzetközi és nemzeti szabályozásai. In: Pintér István (szerk.): Műhelymunkák: A virtuális tér geopolitikája.

Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8.

Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017.

Hautzinger Zoltán: Idegen a büntetőjogban. AndAnn, Pécs, 2016.

Herke Csongor: A műszaki és könyvszakértői vélemény egyes sajátosságai. In: Elek Balázs – Háger Tamás – Tóth Andrea Noémi (szerk.): Igazság, ideál és valóság: Tanulmányok Kardos Sándor 65. születésnapja tiszteletére. Debrecen, 2014. .

Istvanovszki László: A szervezett bűnözés elleni harc új stratégiája és taktikája. Hadtudomány Szemle 2015/1-2.

Kiripovszky Csaba: Az emberkereskedelem és a szervezett bűnözés kapcsolata a prostitúció tükrében. Pécsi Határőr Tudományos Közlemények VIII. Különszám. Pécs, 2007.

MÁTÉ István Zsolt: Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe. Belügyi Szemle 2018/7-8.
MEZEI Kitti – NAGY Zoltán András: The organised criminal phenomenon on the Internet. Journal of Eastern-European Criminal Law 2016/2.
MEZEI Kitti – TÓTH Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós-Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017.
MEZEI Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1.
MEZEI Kitti: Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. JURA 2018/1.
MOLNÁR Gábor: Gazdasági bűncselekmények. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2009.
NAGY Zoltán – MEZEI Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog. 2018/70.
NAGY Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. Belügyi Szemle 2012/6.
NAGY Zoltán András: Bűncselekmények a kibertérben. Ad librum, Budapest, 2009.
NAGY Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! Magyar Jog 2016/1.
NAGY Zoltán András: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1992/1.
NEPARÁCZKI Anna Viktória: A terrorizmus elleni fellépés eszközei a magyar és német büntető anyagi jogban. PhD értekezés. Pécs, 2017.
NYESTE Péter: A nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú stratégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépés területén. Felderítő szemle XII. évfolyam 1. szám 2013.
NYITRAI Endre: A szervezett bűnözés elleni küzdelem büntetőjogi és kriminalisztikai eszközei. PhD értekezés. Pécs, 2017.
PARTI Katalin – KISS Anna: A számítástechnikai bűnözésről akkor és most. In: Bárd Petra – Hack Péter – Holé Katalin: Pusztai László emlékére. OKRI-ELTE ÁJK. Budapest, 2014.
PARTI Katalin: Gyermekpornográfia az interneten. Bíbor Kiadó. Budapest, 2009.
SIMON Béla: A rendészeti szervek együttműködése a kiberbűnözés ellen. Nemzetbiztonsági Szemle 2018/1.
SIMON Béla: Az igazságügyi szakértés egyes kérdései a büntetőeljárásban, különös tekintettel az informatikai szakterületre. Belügyi Szemle 2016/7-8.

Szathmáry Zoltán: A számítástechnikai bűncselekmények. Magyar Jog 2011/3.
Tóth Mihály – Kőhalmi László: A szervezett bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016.
tóth Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009.
Tóth Mihály: XLII. fejezet – A fogyasztók érdekeit és a gazdasági verseny tisztaságát sértő bűncselekmények. In: Tóth Mihály – Nagy Zoltán: Magyar büntetőjog – Különös Rész. Osiris Kiadó. Budapest, 2014.
Urszán József: A szervezett bűnözés fenyegetettség értékelésének jelentősége az Európai Unióban. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Pécsi Tudományos Határőr Közlemények. Pécs, 2013.

HERKE CSONGOR

A DIGITALIZÁCIÓ SZEREPE A BÜNTETŐELJÁRÁSBAN

1. Az elektronikus rendszerek szerepe az 1998. évi XIX. törvényben

A büntetőeljárásról szóló új, 2017. évi XC. törvény (a továbbiakban: Be.) igen sok helyen érinti a büntetőeljárás digitalizációját. Különösen az elektronikus kapcsolattartásnak a résztvevők szélesebb körére való kiterjesztése az, ami lényeges változást eredményez a büntetőeljárásban. Azonban a 2018. június 30-ig hatályos 1998. évi XIX. törvény (a továbbiakban: régi Be.) is számos, a témakört érintő rendelkezést tartalmaz. Ezeket az alábbiak szerint csoportosíthatjuk:

a) vannak általános, a számítógépes kommunikációt illetve technikai rendszert érintő rendelkezések;
b) szólni kell az elektronikus kapcsolattartásra vonatkozó hatályos szabályokról és
c) az elektronikus rendszerekkel összefüggő kényszerintézkedésekről (Információs rendszerben tárolt adatok megőrzésére kötelezés, Elektronikus adat ideiglenes hozzáférhetetlenné tétele);
d) végül meg kell említeni a sajátos különleges eljárásokat is.

ad a) Általánosságban elmondható, hogy éppen a számítógéppel összefüggő kérdések azok, ahol a legtöbb módosítás volt a régi Be. eredeti szövegéhez képest. Lényegében nem találunk olyan §-t a régi Be.-ben, ami a számítógépes környezettel függ össze és az eredeti szöveghez képest ne került volna sor módosításra (többnyire nem is módosításról, hanem utólagos kodifikációról beszélhetünk). Így pl. a 2009. évi LXXXIII. törvény 9. §-a vezette be a Be.-be a „számítógép útján" való idézés lehetőségét (67. § (2) bek.). Ez a „számítógép útján" megjelölés még egyszer előjön a Be.-ben, éspedig ugyanezen törvény tette lehetővé, hogy a nem a kihirdetéskor bejelentett fellebbezést az első fokú bíróságnál számítógép útján is be lehet nyújtani (325. § (3) bek.). Ugyanakkor ennek módjára nem találunk pontos leírást, ami a gyakorlatban komoly problémákat okozhat, így például felmerülnek a következő kérdések:

– Mit tekintünk számítógép útján való előterjesztésnek?
– Mennyiben kell vizsgálni a küldő személyét?
– Az egyéb elektronikus eszközök – pl. mobiltelefon – e tekintetben számítógépnek minősülnek-e? stb.

Szintén az elektronikus rendszerrel összefüggő rendelkezés, miszerint aki az eljárás során keletkezett iratról másolatot kaphat, kérheti, hogy a másolatot a bíróság, az ügyész, illetve a nyomozó hatóság elektronikus úton vagy elektronikus adathordozón adja ki. Ha a bíróságnál, az ügyésznél, illetve a nyomozó hatóságnál a kiadni kért irat elektronikus formában rendelkezésre áll, a másolatot elektronikus úton vagy elektronikus adathordozón kell kiadni. Az így kiadott másolat nem hiteles (70/B. §). Ez a rendelkezés a gyakorlatban akkor jelent problémát, amikor a kiadni kért irat elektronikus formában rendelkezésre áll – ezért a másolatot elektronikus úton vagy elektronikus adathordozón kell kiadni –, ugyanakkor az érintett vagy nem rendelkezik olyan rendszerrel, amivel ezt meg tudja tekinteni (elvárható-e a terhelttől, hogy használjon számítógépet?), vagy objektíve nem képes erre (mert pl. fogva van).

Ha a hatóság állami és helyi önkormányzati szervet, hatóságot, köztestületet, gazdálkodó szervezetet, alapítványt, közalapítványt és egyesületet keres meg adatszolgáltatásra, akkor a 2006. évi LI. törvény által bevezetett módosítás eredményeképpen a megkeresésnek elektronikus úton is eleget lehet tenni (71. §). A 2002. évi I. törvény pedig már azt is lehetővé tette, hogy a tanú a szóbeli kihallgatását követően vagy helyette írásban tegyen vallomást, ami az elektronikus okirat formájában is elkészülhet (ilyenkor azt a tanú minősített elektronikus aláírással látja el, vagy a tanúnak a más módon leírt vallomását bíró vagy közjegyző hitelesíti, 85. § (5) bek.)

Van pár rendelkezés a Be.-ben, ami kifejezetten az elektronikus adat végleges hozzáférhetetlenné tételével (annak lehetőségével) függ össze. Így pl. a 174. § (3) bekezdése értelmében a feljelentést nem lehet elutasítani, ha az elektronikus adat végleges hozzáférhetetlenné tételének a büntethetőségtől függetlenül helye van, kivéve, ha az elektronikus adat végleges hozzáférhetetlenné tételére irányuló eljáráshoz a bizonyítékok rendelkezésre állnak. A 331. § (4) bekezdése szerint, ha a felmentés alapja büntethetőséget kizáró ok, a bíróság az elektronikus adat végleges hozzáférhetetlenné tételét rendelheti el, és a 334. § szerint ennek az eljárásnak a 332. § (1) bekezdés a)-b) és f)-g) pontja alapján történt megszüntetése esetén is helye lehet. Ha ezt a bíróság elmulasztja, akkor másodfokon is helyre lehet hozni, hiszen a 354. § (5) bekezdése szerint, ha az elsőfokú bíróság az elektronikus adat végleges hozzáférhetetlenné tételéről a törvény rendelkezése ellenére nem rendelkezett, a tényállás azonban a döntéshez szükséges adatokat tartalmazza, akkor erről

a másodfokú bíróság is határozhat abban az esetben is, ha a terhelt terhére nem jelentettek be fellebbezést. Ha pedig a másodfokú bíróság az eljárást a 373. § (1) bekezdés I. a) pontja alapján szünteti meg, az elsőfokú bíróság ítéletének az elektronikus adat végleges hozzáférhetetlenné tételére vonatkozó rendelkezését hatályában fenntartja, ha ezekre nézve nem jelentettek be fellebbezést (374. § (1) bek.). Ha pedig az elsőfokú bíróság az elektronikus adat végleges hozzáférhetetlenné tételéről a törvény rendelkezése ellenére nem rendelkezett, és a döntéshez szükséges adatok a másodfokú eljárás során bizonyítás felvétele keretében nem tisztázhatóak, akkor a másodfokú bíróság az elsőfokú bíróságot különleges eljárás lefolytatására utasítja (375. § (4) bek.). Végül meg kell említeni, hogy a 387. § (4) bekezdése alapján a harmadfokú bíróság a megtámadott másodfokú ítéletnek az elektronikus adat végleges hozzáférhetetlenné tételére vonatkozó rendelkezését hivatalból felülbírálja és a másodfokú bíróság ítéletének megváltoztatása esetén határoz az elektronikus adat végleges hozzáférhetetlenné tételéről is (398. § (3) bek.). A külön eljárások körében még szólni kell arról, hogy az 547. § (1) bekezdése alapján a bíróság a tárgyalás mellőzéses végzésben elektronikus adat végleges hozzáférhetetlenné tételét is kimondhatja, de a magánfél emiatt kérheti tárgyalás tartását (548. § (3) bek.). Ha a tárgyalás tartása iránti kérelemben csak az elektronikus adat végleges hozzáférhetetlenné tételére vonatkozó rendelkezést sérelmezték, akkor viszont a bíróság a tárgyaláson csak ebben a kérdésben határoz (549. § (2) bek.).

A régi Be. 200. §-a a titkos adatszerzés egyik módjaként szabályozza a számítástechnikai eszköz vagy rendszer útján továbbított, vagy azon tárolt adatok megismerését, rögzítését és felhasználását (beiktatta a 2010. évi CLXI. törvény 2011. január 1-től). A 202. § (3) bekezdése bizonyos esetekben lehetővé teszi a titkos adatszerzés[1] elrendelését az ügyvéd számítástechnikai rendszer útján történő levelezésére is. A 219. § pedig úgy rendelkezik, hogy a bíróság részére a vádiratot és az elektronikus formában rendelkezésre álló iratokat elektronikus úton is meg kell küldeni, vagy ha ez nem lehetséges, elektronikus adathordozón kell átadni. Ilyenkor a vádirat benyújtásához fűződő joghatások a papír alapon benyújtott vádirat bírósághoz történő beérkezéséhez kötődnek, kivéve, ha az ügyészség a vádiratot minősített elektronikus aláírással látta el, és annak benyújtása a kézbesítési rendszeren keresztül történt.

[1] A régi Be. a nyomozás elrendelését megelőzően folytatott bűnüldözési célú titkos információgyűjtést és a nyomozás elrendelése utáni titkos adatszerzés rendszerét határozta meg, míg az új Be. hatályba lépésével ez megváltozott és a törvény egységesen leplezett eszközöknek nevezi. A leplezett eszközök lehetnek engedélyhez nem kötöttek, valamint engedélyhez kötöttek (ügyészi engedélyhez vagy bírói engedélyhez). Szoros értelemben vett titkos információgyűjtésre – a büntetőeljárási törvény keretein kívül – csak kivételesen kerülhet sor. Lásd Belovics Ervin – Tóth Mihály: Büntető eljárásjog. Harmadik, aktualizált kiadás. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2017. 180. o.

ad b) Az új illetve nagyban módosított 69/A-70. §-ban találunk rendelkezéseket az elektronikus kapcsolattartásra a hatályos Be.-ben. Ezeket a rendelkezéseket azért nem részletezzük, mert 2018. január 1-ével (a 2018. január 1. után indult eljárások tekintetében) a szabályozás lényegében megegyezik a 2017. évi XC. törvény rendelkezéseivel.

ad c) Az információs rendszerben tárolt adatok megőrzésére kötelezés a bűncselekmény felderítése és a bizonyítás érdekében az információs rendszerben tárolt adat birtokosának, feldolgozójának, illetőleg kezelőjének az információs rendszerben tárolt meghatározott adat feletti rendelkezési jogának ideiglenes korlátozását jelenti (158/A. §, a 2013. évi CLXXXVI. törvény által módosított szöveg).

A kényszerintézkedés keretében a bíróság, az ügyész, illetőleg a nyomozó hatóság elrendeli annak az információs rendszerben tárolt adatnak a megőrzését, amely bizonyítási eszköz, vagy bizonyítási eszköz felderítéséhez, a gyanúsított kilétének, tartózkodási helyének a megállapításához szükséges. A megőrzésre kötelezett a határozat vele történő közlésének időpontjától köteles a határozatban megjelölt információs rendszerben tárolt adatot változatlanul megőrizni, és szükség esetén más adatállománytól elkülönítve biztosítani annak biztonságos tárolását. A megőrzésre kötelezett köteles az információs rendszerben tárolt adat megváltoztatását, törlését, megsemmisülését, valamint annak továbbítását, másolat jogosulatlan készítését, illetőleg az adathoz való jogosulatlan hozzáférést megakadályozni.

A megőrzésre kötelezést elrendelő a megőrzéssel érintett adatot fokozott biztonságú elektronikus aláírással láthatja el. Ha az adat eredeti helyen történő megőrzése az érintettnek az adat feldolgozásával, kezelésével, tárolásával vagy továbbításával kapcsolatos tevékenységét jelentősen akadályozná, az elrendelő engedélyével az adat megőrzéséről annak más adathordozóra vagy más információs rendszerbe történő átmásolásával gondoskodhat. Az átmásolást követően az elrendelő az eredeti adatot tartalmazó adathordozóra és információs rendszerre a korlátozásokat részlegesen vagy teljesen feloldhatja.

Ahhoz az adathoz, amelyet a megőrzésre kötelezés érint, az intézkedés tartama alatt kizárólag az elrendelő bíróság, ügyész, illetőleg nyomozó hatóság, valamint az elrendelő engedélyével az adat birtokosa vagy kezelője jogosult hozzáférni. Arról az adatról, amelyet a megőrzésre kötelezés érint, az adat birtokosa vagy kezelője az intézkedés tartama alatt csak az elrendelő kifejezett engedélyével adhat más részére tájékoztatást.

A megőrzésre kötelezett köteles haladéktalanul tájékoztatni az elrendelőt, ha a megőrzésre kötelezéssel érintett adatot jogosulatlanul megváltoztatták, törölték, átmásolták, továbbították, megismerték vagy, hogy ezek megkísérlésére utaló jelet észlelt.

A megőrzésre kötelezést követően az elrendelő haladéktalanul megkezdi az érintett adatok átvizsgálását, és ennek eredményéhez képest az adatnak az információs rendszerbe vagy más adathordozóra történő átmásolásával az adat lefoglalását kell elrendelni, vagy a megőrzésre kötelezést meg kell szüntetni.

A megőrzésre kötelezés az adatot tartalmazó adathordozó lefoglalásáig (az adat átmásolásáig), de legfeljebb három hónapig tart. A megőrzésre kötelezés megszűnik, ha a büntetőeljárást befejezték. A büntetőeljárás befejezéséről a megőrzésre kötelezettet értesíteni kell.[2]

Szintén viszonylag új kényszerintézkedés az elektronikus adat ideiglenes hozzáférhetetlenné tétele (158/B-D. §), amit a 2013. évi LXXVIII. törvény iktatott be a Be.-be 2013. július 1-i hatállyal. Az elektronikus adat ideiglenes hozzáférhetetlenné tétele az elektronikus hírközlő hálózat útján közzétett adat (elektronikus adat) feletti rendelkezési jog ideiglenes korlátozása, és az adathoz való hozzáférés ideiglenes megakadályozása. Ha az eljárás olyan közvádra üldözendő bűncselekmény miatt folyik, amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének van helye, és az a bűncselekmény folytatásának megakadályozásához szükséges, az ideiglenes hozzáférhetetlenné tétel rendelhető el.[3]

Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a bíróság rendeli el az elektronikus adat ideiglenes eltávolításával vagy az elektronikus adathoz való hozzáférés ideiglenes megakadályozásával.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének teljesítésére kötelezett a bíróság megnevezésével és a határozat számának a megjelölésével tájékoztatja a felhasználókat a tartalom eltávolításának vagy a tartalomhoz hozzáférés megakadályozásának a jogalapjáról. Az ideiglenes hozzáférhetetlenné tétel és az információs rendszerben tárolt adatok megőrzésére kötelezés együttesen is elrendelhető.

Az elektronikus adat ideiglenes eltávolítására az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvényben meghatározott tárhelyszolgáltatót kell kötelezni. A kötelezett a határozat vele történő közlését követő egy munkanapon belül köteles az elektronikus adat ideiglenes eltávolítására.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a bíróság megszünteti, és az elektronikus adat visszaállítását rendeli el, ha az ideiglenes hozzáférhetetlenné tétel elrendelésének oka megszűnt, vagy a nyomozást megszüntették, kivéve, ha az

[2] Belovics – Tóth: i.m. 227. o.

[3] Lásd bővebben: Gaiderné Hartmann Tímea: Elektronikus adat ideiglenes és végleges hozzáférhetetlenné tétele – egy új intézmény első évei. Magyar Jog 2015/2. 106-115. o.; valamint Nagy Zoltán András – Mezei Kitti: Az informatikai bűncselekmények. Egyetemi jegyzet. Pécs, 2017. 74-78. o.

elektronikus adat végleges hozzáférhetetlenné tétele elrendelésének lehet helye. Az elektronikus adat ideiglenes hozzáférhetetlenné tétele a büntetőeljárás befejezésével megszűnik. Ha a bíróság az elektronikus adat végleges hozzáférhetetlenné tételét nem rendelte el, az elektronikus adat visszaállítására kötelezi a tárhelyszolgáltatót.

Az ideiglenes hozzáférhetetlenné tétel megszüntetéséről és az elektronikus adat visszaállításáról szóló határozatot a kötelezettel haladéktalanul közölni kell. A tárhelyszolgáltató a határozat vele történő közlésétől számított egy munkanapon belül köteles az elektronikus adat visszaállítására.

Az elektronikus adat ideiglenes eltávolítására és visszaállítására vonatkozó kötelezettség teljesítését a bírósági végrehajtó foganatosítja.

A bíróság hivatalból vagy az ügyész indítványára a tárhelyszolgáltatóval szemben az elektronikus adat ideiglenes eltávolítására vagy visszaállítására vonatkozó kötelezettség elmulasztása miatt százezer forinttól egymillió forintig terjedő rendbírságot szabhat ki. A rendbírság ismételten is kiszabható.

A bíróság elrendeli az elektronikus adat ideiglenes hozzáférhetetlenné tételét, ha:

– a tárhelyszolgáltató az elektronikus adat ideiglenes eltávolítására vonatkozó kötelezettséget nem teljesítette, vagy az elektronikus adat ideiglenes eltávolítására vonatkozóan a külföldi hatóság jogsegély iránti megkeresése a megkeresés kibocsátásától számított harminc napon belül nem vezetett eredményre, és
– a büntetőeljárás bizonyos kiemelt bűncselekményekkel (pl. kábítószer-kereskedelem, gyermekpornográfia, állam elleni bűncselekmény, terrorcselekmény) miatt indult, és az elektronikus adat e bűncselekménnyel áll összefüggésben.

A bíróság a határozatával az elektronikus hírközlési szolgáltatókat kötelezi az elektronikus adathoz való hozzáférés ideiglenes megakadályozására.

Ha az elektronikus adat feletti rendelkezésre jogosult ismeretlen, az elektronikus adat szerinti ideiglenes hozzáférhetetlenné tételéről szóló határozatot hirdetményi úton kell kézbesíteni. A hirdetményt tizenöt napra ki kell függeszteni a bíróság hirdetőtáblájára, továbbá közzé kell tenni a bíróságok központi internetes honlapján. Az elektronikus adat feletti rendelkezésre jogosult a határozattal szemben a kézbesítéstől számított nyolc napon belül fellebbezést jelenthet be.

A bíróság az elektronikus adat ideiglenes hozzáférhetetlenné tétele elrendeléséről elektronikus úton haladéktalanul értesíti a Nemzeti Média- és Hírközlő Hatóságot (a továbbiakban: NMHH). Az elektronikus adat ideiglenes hozzáférhetetlenné tételének a végrehajtását az NMHH szervezi és ellenőrzi. Az NMHH a bíróság elektronikus úton megküldött értesítése alapján az elektronikus adathoz való hoz-

záférés ideiglenes megakadályozására vonatkozó kötelezettséget bevezeti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisába, ezzel egyidejűleg a bíróság határozatáról elektronikus úton haladéktalanul értesíti az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek az elektronikus adathoz való hozzáférés ideiglenes megakadályozására. Ha valamely elektronikus hírközlési szolgáltató a kötelezettséget nem teljesíti, az NMHH erről haladéktalanul értesíti a bíróságot.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a bíróság megszünteti, ha:

– a tárhelyszolgáltató teljesíti az elektronikus adat ideiglenes eltávolítására vonatkozó kötelezettségét,
– az elrendelésének oka egyébként megszűnt, vagy
– a nyomozást megszüntették, kivéve az elektronikus adat végleges hozzáférhetetlenné tétele elrendelésének lehet helye.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének megszüntetéséről a bíróság elektronikus úton haladéktalanul értesíti az NMHH-t, amely az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget törli a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisából, és ezzel egyidejűleg a kötelezettség megszűnéséről elektronikus úton haladéktalanul értesíti az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek biztosítani az elektronikus adathoz a hozzáférést.

Az elektronikus adat ideiglenes hozzáférhetetlenné tétele a büntetőeljárás befejezésével megszűnik. Ha a bíróság az elektronikus adat végleges hozzáférhetetlenné tételét nem rendelte el, az ideiglenes hozzáférhetetlenné tétel megszűnéséről elektronikus úton haladéktalanul értesíti az NMHH-t, amely az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget törli, a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisából, és ezzel egyidejűleg a kötelezettség megszűnéséről elektronikus úton haladéktalanul értesíti az elektronikus hírközlési szolgáltatókat, amelyek az értesítéstől számított egy munkanapon belül kötelesek biztosítani az elektronikus adathoz a hozzáférést. Ha valamely elektronikus hírközlési szolgáltató a hozzáférés újbóli biztosítására vonatkozó kötelezettséget nem teljesíti, az NMHH erről haladéktalanul értesíti a bíróságot.

A bíróság hivatalból vagy az ügyész indítványára az elektronikus hírközlési szolgáltatóval szemben az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vagy a hozzáférés újbóli biztosítására vonatkozó kötelezettség elmulasztása miatt százezer forinttól egymillió forintig terjedő rendbírságot szabhat ki. A rendbírság ismételten is kiszabható.

A 215. § (5) bekezdése szerint fellebbezésre tekintet nélkül végrehajtható az elektronikus adat ideiglenes hozzáférhetetlenné tételének elrendelése.

ad d) A különleges eljárások közül három érinti közvetlenül az elektronikus rendszereket:

– az elkobzásra, a vagyonelkobzásra, az elektronikus adat végleges hozzáférhetetlenné tételére és a lefoglalt dologról történő rendelkezésre irányuló eljárás (569. §);
– az utólagos elkobzás, vagyonelkobzás vagy elektronikus adat végleges hozzáférhetetlenné tétele (570. §) és
– a rendelkezés az elektronikus adat végleges hozzáférhetetlenné tételének a hozzáférés végleges megakadályozásával történő végrehajtásáról (596/A. §).

Az elkobzásra, a vagyonelkobzásra, az elektronikus adat végleges hozzáférhetetlenné tételére és a lefoglalt dologról történő rendelkezésre irányuló eljárás során az ügyész indítványára a bíróság határoz az elektronikus adat végleges hozzáférhetetlenné tételéről, ha büntetőeljárás senki ellen nem indult, vagy azt megszüntették, illetve a terhelt ismeretlen helyen tartózkodása vagy elmebetegsége miatt az eljárást felfüggesztették. A bíróság határozata ellen fellebbezésnek nincs helye, de az ügyész és az, akire a határozat rendelkezést tartalmaz, a végzés kézbesítésétől számított nyolc napon belül tárgyalás tartását kérheti. A tárgyalásról értesíteni kell az ügyészt és az indítvány folytán érdekeltet. Ha az érdekelt ismeretlen, vagy ismeretlen helyen tartózkodik, illetőleg a magyar nyelvet nem ismeri, részére a bíróság képviselőt rendel ki.

Az utólagos elkobzás, vagyonelkobzás vagy elektronikus adat végleges hozzáférhetetlenné tétele elnevezésű különleges eljárásra az elektronikus rendszerrel összefüggésben az ügyész indítványára, illetve hivatalból utólag akkor kerül sor, ha a bíróság jogerős ügydöntő határozatában az elektronikus adat végleges hozzáférhetetlenné tételéről nem vagy nem a törvénynek megfelelően rendelkezett. Ha a bíróság tárgyalást tart, erről az ügyészt, a terheltet, a védőt és az indítvány folytán érdekeltet értesíteni kell. A tárgyaláson hozott végzés ellen az érdekelt is fellebbezhet, a fellebbezésnek halasztó hatálya van.

Legvégül kell megemlíteni az elektronikus adat végleges hozzáférhetetlenné tételének a hozzáférés végleges megakadályozásával történő végrehajtásáról szóló különleges eljárást. Ennek során a bíróság hivatalból vagy az ügyész indítványára az elektronikus adat végleges hozzáférhetetlenné tételének végrehajtását az elektronikus adathoz való hozzáférés végleges megakadályozásával rendeli el, ha:

– a büntetőeljárás befejezésekor az elektronikus adathoz való hozzáférés ideiglenes megakadályozása volt elrendelve és a hozzáférés megakadályozása továbbra is indokolt,

– a tárhelyszolgáltató a kiszabott pénzbírság ellenére nem teljesíti a kötelezettséget,
– az elektronikus adat végleges hozzáférhetetlenné tételét gyermekpornográfia megvalósulása miatt rendelte el, és a tárhelyszolgáltató kötelezettségének nem tesz eleget, a pénzbírság kiszabására tekintet nélkül haladéktalanul,
– az elektronikus adat végleges hozzáférhetetlenné tételére vonatkozóan a külföldi hatóság jogsegély iránti megkeresése a megkeresés kibocsátásától számított harminc napon belül nem vezetett eredményre.

Az elektronikus adat végleges hozzáférhetetlenné tétele végrehajtásának a hozzáférés végleges megakadályozásával történő elrendelése tárgyában hozott határozattal szemben az ügyész a határozat közlésétől, az elektronikus hírközlési szolgáltató az erről szóló értesítéstől és az elektronikus adat feletti rendelkezésre jogosult a határozat közlésétől számított nyolc napon belül fellebbezhet.

A bíróság az ügyész indítványára az elektronikus adat végleges hozzáférhetetlenné tétele végrehajtásának a hozzáférés végleges megakadályozásával történő végrehajtását megszünteti, ha a tárhelyszolgáltató teljesíti az elektronikus adat végleges eltávolítására vonatkozó kötelezettségét.

A bíróság az elektronikus adat végleges hozzáférhetetlenné tételének a hozzáférés végleges megakadályozásával történő elrendeléséről, illetve annak megszüntetéséről szóló határozatáról elektronikus úton haladéktalanul értesíti az NMHH-t. Az elektronikus adat végleges hozzáférhetetlenné tételének a hozzáférés végleges megakadályozásával történő végrehajtását az NMHH szervezi és ellenőrzi.

A bíróság hivatalból vagy az ügyész indítványára az elektronikus hírközlési szolgáltatóval szemben az elektronikus adathoz való hozzáférés végleges megakadályozására vagy a hozzáférés újbóli biztosítására vonatkozó kötelezettség elmulasztása miatt százezer forinttól egymillió forintig terjedő rendbírságot szabhat ki. A rendbírság ismételten is kiszabható. A rendbírságot kiszabó határozattal szemben halasztó hatályú fellebbezésnek van helye.

2. Az elektronikus rendszerek szerepe a 2017. évi XC. törvényben

A Be. jelentősen megváltoztatta a büntetőeljárást mind szerkezeti, mind tartalmi szempontból. Míg a régi Be. a korábbi (szocialista) büntetőeljárási törvények rendszerét követte (alapkoncepciójával ellentétesen), így a hagyományos nyomozás – (közbenső eljárás) – bírósági eljárás rendszerben szabályozta a büntetőeljárást, addig

a hatályos törvény jóval tágabb teret enged a megállapodás alapján folytatott büntetőeljárásnak, illetőleg a terhelt beismerése (tényállás elfogadása) számos egyszerűsítést tesz lehetővé. Ezáltal a büntetőeljárás menete (lehetséges végkimenetele) jóval bonyolultabb, szerteágazóbb, mint a korábban lineáris ábrával leírható eljárásé.

A Be. 23 fejezete közül több is érinti az elektronikus rendszereket. Ezek közül is ki kell emelni az alábbiakat:

1. telekommunikációs eszköz használata (120-126. §)
2. elektronikus kapcsolattartás (148-162. §)
3. kényszerintézkedések:
   – elektronikus adat lefoglalása és a megőrzésre kötelezés (315-317. §)
   – elektronikus adat ideiglenes hozzáférhetetlenné tétele (335-338. §)
4. egyéb, a digitális környezetet érintő Be-rendelkezések.

2.1. A telekommunikációs eszköz használata

A telekommunikációs eszköz használatáról beszélhetünk, ha:

a) az eljárási cselekményen történő jelenlét telekommunikációs eszköz útján is biztosítható
b) az eljárási cselekmény helyszíne és az ettől eltérő helyszín (elkülönített helyszín) között az összeköttetés közvetlenségét és kölcsönösségét
   – kép- és hangfelvétel, vagy
   – folyamatos hangfelvétel (tanú, tolmács, nyomozás során szakértő, terhelt) továbbítása biztosítja.

A telekommunikációs eszköz használatát bármelyik hatóság elrendelheti, akár hivatalból, akár az érintett indítványára. Az indítvány elutasítása és általában annak elrendelése ellen nincs helye jogorvoslatnak.

A telekommunikációs eszköz használatát kötelező elrendelni a különleges bánásmódot igénylő sértettnél és a fogva lévő (személyi védelem alatt álló, Védelmi Programban részt vevő) tanú vagy terhelt esetén (kivéve, ha a cél más módon is biztosítható vagy az érintett személyes megjelenése nélkülözhetetlen). Ugyanakkor csak a terhelt hozzájárulásával rendelhető el a személyi szabadságot érintő bírói engedélyes kényszerintézkedés elrendelése tárgyában tartott ülésen és az előkészítő ülésen (a terhelti jelenlét biztosítására).

A telekommunikációs eszköz használata során az alábbi személyek vehetnek részt:

– akinek a jelenlétét a telekommunikációs eszköz útján biztosítják,
– a védője vagy segítője,
– a hatóság tagja,

– fogvatartott személy esetében a fogvatartott személyazonosságának megállapítására feljogosított dolgozó és a terhelt őrzését ellátó személy,
– a szakértő,
– a telekommunikációs eszköz működését biztosító személyzet.

A telekommunikációs eszköz használata során a hatóság (akár a bv. személyzet közreműködésével) megállapítja az elkülönített helyszín címét, az ott jelen lévő személyek személyazonosságát és személyes adatait, és ellenőrzi, hogy az elkülönített helyszínen jogosulatlan személy nem tartózkodik. Ez a sajátos eljárás sem sértheti a kérdezési, észrevételezési, indítványtételi és egyéb eljárási jogokat. Ez különösen akkor merülhet fel, ha a terhelt a védőjével nem egy helyszínen tartózkodik. Ilyenkor közöttük a tanácskozást legalább hangkapcsolatot biztosító elektronikus úton kell lehetővé tenni.

Biztosítani kell a telekommunikációs eszköz használata során, hogy az eljárási cselekményen jelen lévő személyek lássák és hallják az elkülönített helyszínen jelen lévő személyeket, akik pedig követhessék az eljárási cselekmény menetét.

A különleges bánásmódot igénylő személy érdekében elrendelhető, hogy:
– az érintett az eltérő helyen jelen lévő terheltet ne láthassa, illetve hallhassa
– a személyazonosság megállapítására alkalmas egyedi tulajdonságokat technikai eszközzel torzítsák.

Telekommunikációs eszköz használata esetén a jegyzőkönyv az alábbiakat tartalmazza:
– a használat ténye és módja,
– annak megjelölése, akinek a jelenlétét biztosítják,
– az elkülönített helyszín címe,
– az elkülönített helyszínen tartózkodó egyéb személyek neve és hogy milyen minőségben vannak jelen.

2.2. Az elektronikus kapcsolattartás

A Be. igen széles körben teszi lehetővé (és kötelezővé) az elektronikus kapcsolattartást[4]. Mivel ez a résztvevők közül elsősorban a védőt érinti, ezért a vizsgálat során van először igazán jelentősége.

[4] Lásd ehhez: Csák Zsolt: XXVII. fejezet – Az elektronikus kapcsolattartás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018.; Bartkó Róbert: Elektronikus kapcsolattartás a büntetőeljárásban. In: Karácsony Gergely (szerk.): Az elektronikus eljárások joga. Gondolat Kiadó. Budapest, 2018. 73-99. o.

Az E-ügyintézési törvény (2015. évi CCXXII. tv.) 17. § (1) bekezdése szabályozza az elektronikus kapcsolattartás során alkalmazott jognyilatkozat megfelelőségét. Eszerint ennek két feltétele van:

– a nyilatkozattevő elektronikus azonosítása megfelelően történik (elektronikus azonosítási szolgáltatással, megfelelő elektronikus azonosító eszközzel (eIDAS) vagy az elektronikus ügyintézést biztosító szerv által megfelelővé nyilvánított elektronikus azonosítási szolgáltatás útján) és
– biztosított, hogy a kézbesített elektronikus dokumentum megegyezik a nyilatkozattevő által jóváhagyott dokumentummal.

A megfelelő elektronikus azonosító eszköz (eIDAS Rendelet: 910/2014/EU-rendelet 6. cikk (1) bekezdés) a kölcsönös elismerés alapján: mindegyik tagállamban kibocsátott, elfogadott elektronikus azonosító eszközt el kell ismerni a más tagállamban, ha:

– az elektronikus azonosító eszközt a Bizottság által a 9. cikkel összhangban közzétett listában szereplő valamelyik elektronikus azonosítási rendszer keretében bocsátották ki,
– az elektronikus azonosító eszköz biztonsági szintje „jelentős" vagy „magas", és azonos vagy magasabb, mint az adott tagállamban előírt biztonsági szint,
– az érintett közigazgatási szerv a „jelentős" vagy „magas" biztonsági szintet használja az online hozzáféréssel kapcsolatban.

Az elektronikus kapcsolattartásnak az alábbi fajtái vannak:

Választható elektronikus kapcsolattartás (149. §)	– a nem kötelezett résztvevő/jogi képviselőnek nem minősülő képviselője vállalja – az elektronikus jognyilatkozat megfelelősége – a hatósággal a kapcsolatot elektronikus úton kell tartani/a hatóság is elektronikus úton kézbesít neki – ha a hatóság papíralapon kézbesít, a címzettet tájékoztatja, hogy elektronikus úton is tarthat kapcsolatot – nyilatkozat hiányában benyújtott beadvány: a hatóság elektronikus úton figyelmezteti, hogy a továbbiakban a kapcsolatot elektronikus úton az erre vonatkozó nyilatkozat megtételével tarthatja
Kötelező elektronikus kapcsolattartás (150. §)	– a kötelezett résztvevő minden beadványt kizárólag elektronikus úton nyújthat be a hatósághoz + a hatóság is elektronikus úton kézbesít a részére – mentesül a kötelező elektronikus kapcsolattartás alól, akinek elektronikus ügyintézéshez való joga szünetel

Elektronikus kapcsolattartás a szakértővel (151. §)	– általában az elektronikus kapcsolattartásra kötelezett szakértőre vonatkozik – az elektronikus kapcsolattartásra nem kötelezett szakértő is vállalhatja az elektronikus kapcsolattartást: • az igazságügyi szakértői névjegyzékbe történő bejelentéssel • itt nem szereplő szakértő: a hatóságnak való bejelentéssel – az elektronikus kapcsolattartásra köteles (azt vállaló) szakértő a szakvéleményét (egyéb beadványát) elektronikus úton nyújthatja be a hatósághoz/a hatóság is valamennyi ügyiratot elektronikus úton kézbesít a részére – a papíralapú kapcsolattartással eljáró szakértő felhívható arra, hogy a szakvéleményt adathordozón is nyújtsa be, ha azt elektronikus úton kell kézbesíteni
A hatóságok egymás közötti és más szervekkel történő elektronikus kapcsolattartása (152. §)	– a hatóságok elektronikus úton tartják a kapcsolatot egymással + törvény alapján elektronikus ügyintézést biztosító szervvel + a Kormány által kijelölt közfeladatot ellátó szervvel

A meghatalmazott védőnek és jogi képviselőnek elektronikus kapcsolattartás esetén az első beadvány mellékleteként csatolnia kell az elektronikus okiratként rendelkezésre álló vagy általa digitalizált meghatalmazást (kivéve, ha a meghatalmazása a rendelkezési nyilvántartásban szerepel). A hatóság az eredeti meghatalmazás bemutatására hívhatja fel (az egyezőség megállapítása érdekében). A képviselettel bíró, de elektronikus útra nem köteles résztvevő a meghatalmazás visszavonására irányuló nyilatkozatát papíralapon is benyújthatja (és nyilatkozik arról, hogy a továbbiakban lesz-e védője vagy jogi képviselője; ha lesz, ezt a meghatalmazást is csatolni kell).

Papíralapú okiratok esetén, ha elektronikus kapcsolattartás áll fenn, a résztvevő maga köteles gondoskodni a digitalizálásról és a papíralapú irat megőrzéséről. Ha erre nem kerül sor, a hatóság 10 munkanapon belül digitalizálja azt. Ha azonban be kell mutatni a papíralapú iratot, akkor nem kell elektronikusan is benyújtani.

Az elektronikus kapcsolattartás biztosítása céljából érkezett adatok kezelésére jogosult szerv:

– az Országos Bírósági Hivatal,
– a bíróság,
– az ügyészség és
– a nyomozó hatóság.

Az elektronikus kapcsolattartással összefüggésben kell szólni az elektronikus formátumban rendelkezésre álló ügyirat[5] továbbításáról az elektronikus levelezési címre. Ezt a résztvevő indítványozhatja, ha az ügyirat a hatóságnál rendelkezésre áll. Ilyenkor az ügyiratot elektronikus formában, elektronikus okiratként vagy a papíralapú okirat elektronikus másolataként kell részére továbbítani (159. §). Ilyenkor az ügyirat továbbításáért nem kell illetéket fizetni.

Az elektronikus kapcsolattartásra vonatkozó egyéb szabályok:

– legkésőbb a határidő utolsó napján kell elektronikus úton benyújtani az iratokat (nem munkaidőben!), amibe nem számít bele az a nap, amely során legalább négy órán át jogszabályban meghatározottak szerinti üzemzavar (üzemszünet) állt fenn;
– ha a résztvevő nem vállalja az elektronikus kapcsolattartást, a papíralapú beadványát (ha azt elektronikus kapcsolattartással eljáró résztvevő részére kell kézbesíteni) a hatóság digitalizálja és azt elektronikus úton kézbesíti a másik résztvevő számára + részére papíralapon kézbesítik az ügyiratot akkor is, ha az eljárásban jogi képviselője (elektronikus kapcsolattartást vállaló egyéb képviselője) útján jár el, de az ügyiratot nem a képviselő részére kell kézbesíteni, vagy a képviselő részére nem lehet kézbesíteni;
– a hatóság az elektronikus úton kézbesített ügyiratot minősített/minősített tanúsítványon alapuló elektronikus aláírással vagy elektronikus bélyegzővel látja el, és ez közokirat;
– a hatóság az ügyirat megismerésére jogosultak számára biztosítja az ügyiratokhoz való elektronikus hozzáférés lehetőségét;
– az elektronikus úton tett nyilatkozat hatálytalan, ha a feltételeknek nem felel meg;
– ha az elektronikus úton kapcsolatot tartó a beadványát nem elektronikus úton/elektronikus úton, de nem megfelelően nyújtotta be:
  • a jogorvoslatot a hatóság érdemi indokolás nélkül elutasítja;
  • a beadványban foglalt egyéb nyilatkozat hatálytalan;
– ha az ügyirat azért nem kézbesíthető, mert az elektronikus úton kapcsolatot tartó az elektronikus kapcsolattartáshoz szükséges szolgáltatásokkal nem ren-

[5] A Be. nem határozza meg az ügyirat definícióját, azonban 100. § (2) bekezdése támpontot ad, amely szerint ügyiratnak minősülnek a bíróság, az ügyészség és a nyomozó hatóság által beszerzett, illetve a büntetőeljárásban részt vevő személyek által benyújtott, valamint csatolt iratok és a további bizonyítási eszközök. Ezek lehetnek hagyományos papíralapú iratok, valamint bűnjelként kezelt kép-, hang-, illetve kép- és hangfelvételek, valamint az egyéb, bármilyen formátumban rendelkezésre álló elektronikus dokumentumok. Lásd ehhez bővebben: Tisza-Papp Judit: Elektronikus ügyirat a büntetőeljárásban. Fontes Iuris 2018/2. 28-31. o.

delkezik, a hatóság az ügyiratot papír alapon kézbesíti (de ekkor az érintett rendbírsággal sújtható);
– ha az érintett vállalta, hogy a kapcsolatot elektronikus úton tartja, utóbb, beadványának papíralapú benyújtásával egyidejűleg indítványozhatja a hatóságnál a papíralapú eljárásra való áttérés engedélyezését, amennyiben valószínűsíti, hogy a körülményeiben olyan változás következett be, amely miatt az elektronikus úton történő eljárás a továbbiakban számára aránytalan megterhelést jelentene (az engedélyezésről nem is kell formális határozatot hozni);
– a hatóság papíralapon tartja a kapcsolatot/papíralapú kapcsolattartásra tér át, ha a résztvevő elektronikus ügyintézéshez való joga szünetel.

2.3. A kényszerintézkedések

A kényszerintézkedések közül kettő van, ami kifejezetten a digitális környezettel függ össze:

a) elektronikus adat lefoglalása és a megőrzésre kötelezés (315-317. §)[6]
b) elektronikus adat ideiglenes hozzáférhetetlenné tétele (335-338. §)

ad a) Amennyiben a büntetőeljárás érdekében elektronikus adat lefoglalására van szükség, általában nem kell az elektronikus adatot tartalmazó információs rendszert (számítógépet, szervert) vagy adathordozót lefoglalni. Ennek oka az, hogy a bizonyítás szempontjából magának az adatnak van relevanciája, amit számos más módon is ki lehet nyerni az elektronikus adatot tartalmazó információs rendszerből vagy adathordozóból (másolat, adatáthelyezés). A másolat történhet úgy, hogy ha a nyomozó hatóság (esetleg szaktanácsadó igénybevételével) pontosan tudja, melyik adatokra van szükség az adott elektronikus adatot tartalmazó információs rendszerből (adathordozóból), akkor csak azt másolja le. Ha ez a lefoglalás időpontjában pontosan nem körülhatárolható, akkor mód van a teljes tartalom átmásolására. A lefoglalás a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról szóló 11/2003. (V. 8.) IM-BM-PM együttes rendelet 67. §-a szerint az átmásolás utólag meg nem változtatható adathordozóra történhet. Az átmásolást megelőzően a lefoglalás helyszínén ellenőrizni kell, hogy a hatóság által az átmásoláshoz biztosított adathordozó adatokat nem tartalmaz. Az átmásolás során biztosítani kell azt, hogy az eredeti adatok ne változzanak meg. A hatóság a jegyzőkönyvben a rögzítésre használt adathordozó típusát, gyártási számát, illetőleg a rajta tárolt adat jellegét és tartalmát feltünteti.

[6] Ezekről bővebben: Czine Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018.

De az is lehetséges, hogy felmerül a gyanú, hogy az adathordozó olyan (pl. már törölt) adatokat is tartalmaz, amelyek az egyszerű másolással nem foglalhatók le. Ilyenkor kerülhet sor az elektronikus adatot tartalmazó információs rendszer (adathordozó) lefoglalására, mivel a szakértő az eredeti eszközről kinyerheti ezeket a törölt (esetleg tikosított) adatokat is. Szintén sor kerülhet az adott elektronikus adatot tartalmazó információs rendszer (adathordozó) fizikai lefoglalására, ha az bizonyítási eszköz, illetőleg elkobozható vagy vagyonelkobzás alá esik. Mivel a 315. § (4) bekezdése szerint az elektronikus adat lefoglalását úgy kell végrehajtani, hogy az a büntetőeljárás céljából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, ezért ha az elektronikus adatot tartalmazó információs rendszer (adathordozó) fizikai lefoglalására kerül sor, akkor meg kell indokolni, hogy ennek mi az oka, miért nem elegendő az egyszerű vagy teljes másolat készítése.

A fizetésre használt elektronikus adat esetén elegendő lehet, ha megakadályozzák, hogy a lefoglalást elszenvedő ezt az adatot fizetésre használja. Be. 315. §-ban alakította ki az ún. virtuális vagyontárgyak biztosításának a keretszabályait, amely alapján a virtuális fizetőeszközök mint a bitcoin és az elektronikus pénz is a lefoglalás tárgyát képezheti.[7] Ezért ilyenkor az is lehetséges lefoglalási mód, hogy a fizetésre használt elektronikus adat felhasználhatóságát akadályozzák meg (akár rossz kódok megadásával zárolva, akár az adat tartalmát letéti számlára utalva stb.).

Az irat lefoglalásához hasonlóan az információs rendszer vagy adathordozó lefoglalása esetén az elektronikus adattal rendelkezni jogosult kérésére másolatot kell készíteni az általa megjelölt elektronikus adatról, de csak akkor, ha ez az eljárás érdekét nem veszélyezteti.

Elektronikus adat esetén is előfordulhat, hogy a lefoglalást (az érintett őrizetében hagyással történő lefoglalás analógiájára) úgy rendelik el, hogy sem (teljes) másolat útján, sem az adott elektronikus adatot tartalmazó információs rendszer (adathordozó) fizikai lefoglalásával nem foganosítják, hanem az elektronikus adat birtokosának, feldolgozójának, kezelőjének (együtt: a megőrzésre kötelezettnek) az elektronikus adat feletti rendelkezési jogát korlátozzák. Ilyenkor a határozat kézbesítését követően a megőrzésre kötelezettnek kell ügyelnie arra, hogy az adatot sem ő, sem más ne változtassa meg (törölje, semmisítse meg, továbbítsa, jogosulatlanul másolatot készítsen, az adathoz jogosulatlanul hozzáférjen). A megőrzésre kötelezett indítványára az is elrendelhető, hogy ne kelljen az adott elektronikus adatot fizikailag ott megőriznie, ahol a hatóság azt fellelte, hanem az elektronikus adatról

[7] Mezei Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. Magyar Jogászegyleti Értekezések 9-10. Budapest, 2018. 172. o.; Lásd még: Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/11. 639-647. o.

másolatot készítsen, és azt őrizze meg. Ilyenkor az eredeti elektronikus adatot (ha a határozat erre engedélyt ad) már akár meg is változtathatja a megőrzésre kötelezett.

A megőrzésre kötelezést elrendelő a megőrzéssel érintett elektronikus adatot minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírással vagy elektronikus bélyegzővel láthatja el, de ez nem kötelező. A fokozott biztonságú elektronikus aláírás az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 1. § 22. pontja értelmében az eIDAS Rendelet (az Európai Parlament és a Tanács 2014. július 23-i 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről) 3. cikkének 11. pontja szerint olyan elektronikus aláírás, amely megfelel a 26. cikkben meghatározott követelményeknek:

– kizárólag az aláíróhoz köthető;
– alkalmas az aláíró azonosítására;
– olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
– olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Előfordulhat, hogy a megőrzésre kötelezett legnagyobb gondossága ellenére is valaki hozzáfér az adathoz (pl. hackertámadás). Ilyenkor nyilvánvalóan nem várható el a megőrzésre kötelezettől, hogy az általánosan elvárható mértéken felül megakadályozza, hogy az adatot egy kívülálló megváltoztassa (letörölje, megsemmisítse, továbbítsa, jogosulatlanul másolatot készítsen, az adathoz jogosulatlanul hozzáférjen). Ugyanakkor a megőrzésre kötelezett köteles haladéktalanul tájékoztatni a megőrzésre kötelezést elrendelőt, ha a megőrzésre kötelezéssel érintett elektronikus adatot jogosulatlanul megváltoztatták, törölték, megsemmisítették, továbbították, átmásolták, megismerték, vagy ezek megkísérlésére utaló jelet észlelt.

A megőrzésre kötelezés a védelőkészítéssel, a nyomozás törvényessége feletti felügyelettel és a vádemeléssel kapcsolatos ügyészi feladatokról szóló 11/2003. (ÜK. 7.) LÜ utasítás 28/A. §-a alapján elrendelésére az ügyész tesz indítványt a nyomozási bíróhoz. Az indítványban a kényszerintézkedéssel érintett elektronikus adatot és a kötelezett szolgáltatót meg kell határozni. Ha az ügyész a kényszerintézkedés elrendelését követően észleli, hogy a kényszerintézkedés hatálya alá tartozó elektronikus adat változatlanul hozzáférhető, a rendbírság kiszabására irányuló indítvány megtétele előtt az ügyésznek a 28/A. § (2) bekezdése szerint meg kell győződnie arról, hogy az elérés azért lehetséges-e, mert a bíróság által kötelezett tárhelyszolgál-

tató vagy elektronikus hírközlési szolgáltató a kötelezettségét nem teljesítette. Ha az elérést más tárhelyszolgáltató vagy elektronikus hírközlési szolgáltató biztosítja, új kényszerintézkedés elrendelése iránt indokolt intézkedni.

A megőrzésre kötelezés legfeljebb három hónapig tart és csak a büntetőeljárás alatt kerülhet rá sor.

A 308. § (3) bekezdése értelmében az elektronikus adat is a lefoglalható tárgyak közé tartozik, ezért értelemszerűen alkalmazni kell rá a lefoglalt dolog megváltására, értékesítésére és elkobzására, valamint a lefoglalás megszüntetésére és visszatartására vonatkozó rendelkezéseket.

ad b) Az elektronikus adat ideiglenes hozzáférhetetlenné tétele a végleges hozzáférhetetlenné tételt (Btk. 77. §) biztosító, csak a bíróság által elrendelhető kényszerintézkedés. Ennek két módja van (amelyek akár együttesen is elrendelhetők): az elektronikus adat ideiglenes eltávolítása és az adathoz való hozzáférés ideiglenes megakadályozása.

Az elektronikus adat ideiglenes hozzáférhetetlenné tételének végrehajtási szabályait a bírósági végrehajtásról szóló 1994. évi LIII. törvény 201/C. §-a tartalmazza. Eszerint az elektronikus adat ideiglenes hozzáférhetetlenné tételéről szóló határozatot a bíróság megküldi a végrehajtónak. A végrehajtó a határozatot személyesen kézbesíti a kötelezettnek, és ellenőrzi a kötelezett azonnali teljesítését a helyszínen, illetve ha az azonnali teljesítés feltételei nem állnak fenn, a végrehajtó legkésőbb a kézbesítést követő munkanapon ellenőrzi a helyszínen a teljesítést. Ha a végrehajtó az ellenőrzés során azt állapítja meg, hogy a kötelezett nem teljesítette a kötelezettséget, erről haladéktalanul jegyzőkönyvet készít, és azt legkésőbb a jegyzőkönyv készítésének napját követő munkanapon beterjeszti az elektronikus adat ideiglenes hozzáférhetetlenné tételét vagy visszaállítását elrendelő bírósághoz rendbírság kiszabása céljából. Ha az elektronikus adat ideiglenes hozzáférhetetlenné tételének elrendelése esetén a rendbírság kiszabását követően a kötelezett teljesít, és erről a végrehajtót értesíti, a végrehajtó az értesítés átvételét követő öt munkanapon belül ismételten (szükség esetén a helyszínen) ellenőrzi a kötelezett teljesítését, és az ellenőrzés eredményéről haladéktalanul tájékoztatja az azt elrendelő bíróságot.

Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § l) pontja szerint közvetítő szolgáltató az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely

– az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel és hozzáférés-biztosítás);

– az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolás);
– az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltatás);
– információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatás);
– alkalmazásszolgáltató.

Őket együttesen nevezi a 336. § (1) bekezdése eltávolításra kötelezettnek, aki a határozat vele történő közlését követő egy munkanapon belül köteles az elektronikus adat ideiglenes eltávolítására.

Az elektronikus adatot a határozat közlésétől számított egy munkanapon belül vissza kell állítani, ha az elrendelésének oka megszűnt, vagy az eljárás a Btk. 77. § (2) bekezdése szerinti elektronikus adat végleges hozzáférhetetlenné tétele nélkül fejeződött be.

A bíróság hivatalból vagy az ügyészség indítványára az eltávolításra kötelezettet az elektronikus adat ideiglenes eltávolítására vagy visszaállítására vonatkozó kötelezettség elmulasztása miatt rendbírsággal sújthatja.

A bíróság bizonyos kiemelt bűncselekmények miatt folyó büntetőeljárásokban az elektronikus hírközlési szolgáltatókat kötelezheti az elektronikus adathoz való hozzáférés ideiglenes megakadályozására, ha az elektronikus adat ideiglenes eltávolítására a határozat ellenére nem került sor. Az elektronikus adat felett rendelkezésre jogosultnak ezt a határozatot kézbesíteni kell (ha ismert), aki a határozattal szemben a kézbesítéstől számított nyolc napon belül fellebbezést jelenthet be. A bíróság az elektronikus adathoz való hozzáférés ideiglenes megakadályozásának elrendelését haladéktalanul közli a Nemzeti Média- és Hírközlési Hatósággal, amely a kényszerintézkedés végrehajtását szervezi és ellenőrzi. A Nemzeti Média- és Hírközlési Hatóságra vonatkozó alapvető szabályokat a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény Negyedik Része tartalmazza.

A NMHH a hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget bevezeti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisába, ezzel egyidejűleg a bíróság határozatáról elektronikus úton haladéktalanul tájékoztatja az elektronikus hírközlési szolgáltatókat, amelyek a tájékoztatástól számított egy munkanapon belül kötelesek az elektronikus adathoz való hozzáférés ideiglenes megakadályozására.

A bíróság hivatalból vagy az ügyészség indítványára az elektronikus hírközlési szolgáltatót az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vagy a hozzáférés újbóli biztosítására vonatkozó kötelezettség elmulasztása miatt rendbírsággal sújthatja.

A védelőkészítéssel, a nyomozás törvényessége feletti felügyelettel és a vádemeléssel kapcsolatos ügyészi feladatokról szóló 11/2003. (ÜK. 7.) LÜ utasítás 28/A. § (2) bekezdése szerint, ha az ügyész a kényszerintézkedés elrendelését követően észleli, hogy az elektronikus adat változatlanul hozzáférhető, a rendbírság kiszabására irányuló indítvány megtétele előtt meg kell, hogy győződjön arról, hogy az elérés azért lehetséges, mert a bíróság által kötelezett tárhelyszolgáltató vagy elektronikus hírközlési szolgáltató a kötelezettségét nem teljesítette. Ha az elérést más tárhelyszolgáltató vagy elektronikus hírközlési szolgáltató biztosítja, új kényszerintézkedés elrendelése (és nem a rendbírság) iránt indokolt intézkedni. A bírósági végrehajtásról szóló 1994. évi LIII. törvény 201/C. §-a alapján az elektronikus adathoz való hozzáférés ideiglenes megakadályozásáról szóló határozatot a bíróság megküldi a végrehajtónak. A végrehajtó a határozatot személyesen kézbesíti a kötelezettnek, és ellenőrzi a kötelezett azonnali teljesítését a helyszínen, illetve ha az azonnali teljesítés feltételei nem állnak fenn, a végrehajtó legkésőbb a kézbesítést követő munkanapon ellenőrzi a helyszínen a teljesítést. Ha a végrehajtó az ellenőrzés során azt állapítja meg, hogy a kötelezett nem teljesítette a kötelezettséget, erről haladéktalanul (a teljesítési határidő lejártának napját is tartalmazó) jegyzőkönyvet készít, és azt legkésőbb a jegyzőkönyv készítésének napját követő munkanapon beterjeszti az elektronikus adathoz való hozzáférés ideiglenes megakadályozását elrendelő bírósághoz rendbírság kiszabása céljából. Ha az elektronikus adathoz való hozzáférés ideiglenes megakadályozásának elrendelése esetén a rendbírság kiszabását követően a kötelezett teljesít, és erről a végrehajtót értesíti, a végrehajtó az értesítés átvételét követő öt munkanapon belül ismételten (szükség esetén a helyszínen) ellenőrzi a kötelezett teljesítését, és az ellenőrzés eredményéről haladéktalanul tájékoztatja az azt elrendelő bíróságot.

A hozzáférés ideiglenes megakadályozása megszűnik, ha elrendelésének oka megszűnt vagy az eljárás a Btk. 77. § (2) bekezdése szerinti elektronikus adat végleges hozzáférhetetlenné tétele nélkül fejeződött be.

Az elektronikus adat önkéntes eltávolítása érdekében való felhívás sajátos kényszerintézkedés, hiszen teljesítése nem kötelező. Célja mindössze az elektronikus adathoz való hozzáférés megakadályozásának a gyorsabbá tétele.

2.4. A Be. egyéb rendelkezései

A Be. számos olyan egyéb rendelkezést tartalmaz, amely érinti a digitális környezetet. Ezeket nem kívánjuk részletezni, csak néhányat felsorolunk közülük:

- digitális védői meghatalmazás (45. §);
- a személyes adatok zártan kezelésének az összefüggései az elektronikus rendszerrel (99. §);
- elektronikus idézés és értesítés (113. és 116. §);

– elektronikus kézbesítés (130., 132. és 135. §);
– írásbeli tanúvallomás elektronikus környezetben (181. §);
– egyes bizonyítékok[8] (elektronikus adat, 205. §; hozzájárulással alkalmazott megfigyelés, 220. §; információs rendszer titkos megfigyelése, 232. §; elektronikus adatkérés 261. §);
– elektronikus adat végleges hozzáférhetetlenné tétele (570., 609. és 741. §);
– eljárás adat hozzáférhetetlenné tétele érdekében (819-820. §);
– egyszerűsített felülvizsgálati eljárás az elektronikus adat végleges hozzáférhetetlenné tételével kapcsolatosan (672. §).

Felhasznált Irodalom

Bartkó Róbert: Elektronikus kapcsolattartás a büntetőeljárásban. In: Karácsony Gergely (szerk.): Az elektronikus eljárások joga. Gondolat Kiadó. Budapest, 2018.

Belovics Ervin – Tóth Mihály: Büntető eljárásjog. Harmadik, aktualizált kiadás. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2017.

Czine Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018.

Csák Zsolt: XXVII. fejezet – Az elektronikus kapcsolattartás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018.

Gaiderné Hartmann Tímea: Elektronikus adat ideiglenes és végleges hozzáférhetetlenné tétele – egy új intézmény első évei. Magyar Jog 2015/2.

Mezei Kitti: A kiberbűncselekmények hazai szabályozásának aktuális kérdései. Magyar Jogászegyleti Értekezések 9-10. Budapest, 2018.

Nagy Zoltán András – Mezei Kitti: Az informatikai bűncselekmények. Egyetemi jegyzet. Pécs, 2017.

Szabó Imre: A számítástechnikai adat mint elektronikus bizonyíték. Kriminológiai Tanulmányok 48. OKRI, Budapest, 2011.

Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/11.

Tisza-Papp Judit: Elektronikus ügyirat a büntetőeljárásban. Fontes Iuris 2018/2.

[8] Szabó Imre: A számítástechnikai adat mint elektronikus bizonyíték. Kriminológiai Tanulmányok 48. OKRI, Budapest, 2011. 13-28. o.

MEZEI KITTI

A SZERVEZETT BŰNÖZÉS AZ INTERNETEN[1]

1. Bevezetés

Az internet vonzó környezetté vált a különböző profit-orientált bűnelkövetők számára, különösen mert a határokon átível, magasfokú anonimitást biztosít és nincs szükség arra, hogy jelen legyenek fizikailag a bűncselekmények elkövetésének a helyszínén, ezért a kockázat minimalizálása mellett jelentős profitra tudnak szert tenni.[2] Ez különösen kedvező, ha olyan országokból tudják működtetni a bűnözői infrastruktúrájukat, ahol nem biztosított a megfelelő jogszabályi háttér és technológiai kapacitás sem ahhoz, hogy hatékonyan feltudjanak lépni például az informatikai vagy másnéven kiberbűncselekményekkel[3] szemben.

A technológiai fejlődést kihasználó bűnelkövetők tevékenysége két csoportra osztható: egyrészt vannak az olyan büntetendő magatartások, amelyek korábban is léteztek, de az internetes kapcsolattartási és más lehetőségek jobban elősegítik azok terjedését, így akár nagyságrendileg is növelve a társadalmi veszélyességüket. Ide so-

[1] Az Emberi Erőforrások Minisztériuma ÚNKP-17-3-I kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

[2] Gyaraki Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények – A PIN kód megadása sikeres vagy biztonságos az internet?! Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012. 235. o.

[3] A szakirodalom szerinti informatikai bűnözésre vagy kiberbűnözésre (cybercrime) mint egy gyűjtőfogalomként lehet tekinteni, amelynek két fő csoportja különböztethető meg: az egyik azon deliktumok csoportja, amelyek kizárólag információs rendszerekkel (számítógépekkel, azok hálózatával vagy egyéb ICT eszköz használatával) követhetők el. Jellemzően ezeknek a bűncselekményeknek a tárgya az információs rendszer, tehát amikor a támadás ez ellen irányul. Ezek a tisztán informatikai bűncselekmények vagy kiberbűncselekmények, az ún. „cyber-dependent crime" (pl. számítógépes vírusok használata, hacking stb.). A második tágabb kategóriába tartoznak azok a hagyományos bűncselekmények, amelyeket az információs rendszerek felhasználásával valósítanak meg mint például ilyen a csalás, zsarolás, gyermekpornográfia, szerzői jogi jogsértések, zaklatás stb., ez az ún. „cyber-enabled crime" esetköre, amikor az információs rendszer a bűncselekmény elkövetésének az eszköze. Lásd Clough, Jonathan: Principles of Cybercrime. Cambridge University Press, 2015. 10-11. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assess-ment-iocta-2017 [2018.03.14.]

rolhatók mindenekelőtt a szervezett bűnözés hagyományos „üzletágai" (pl. kábítószer-kereskedés) és másrészről vannak azok, amelyek a már említett módon a technológiai vívmányok nélkül nem léteznének mint a kiberbűncselekmények köre.[4]

Kétségtelen tény, hogy a hagyományos szervezett bűnözői csoportok számára is kedvezővé vált a modern technológiák használata, azonban az kérdéses, hogy milyen mértékben terjed ki a tevékenységi körük például a kiberbűnözésre. Jellemző rájuk, hogy az ún. bűnözői feketegazdaságban[5] fejtik ki a különféle illegális tevékenységüket – melyet a kereslet-kínálat törvénye határoz meg –, és ezt is megkönnyíti számukra, hogy a valós téren kívül már a digitális platformokon keresztül is folytathatják ezt. Nem véletlen, hogy a szervezett bűnözés motorját napjainkban már az illegális online kereskedelem jelenti. A szervezett bűnözés és a kiberbűnözéssel kapcsolatban két kérdés merül fel:

– az internet egy új színteret jelent-e a tradicionális szervezett bűnözői csoportok számára a különböző illegális tevékenységük folytatásához és/vagy
– lehetőséget teremt az új típusú, „szervezett" kiberbűnözői csoportok működéséhez, amelyek kifejezetten a kiberbűncselekmények elkövetésére specializálódnak.

2. A szervezett bűnözés fogalma és a hazai szabályozás

A szervezett bűnözői csoportok működését és értékrendjét meghatározzák azok az országok, társadalmak, illetve kultúrák, amelyekben tevékenységüket kifejtik, így különösen hatással van a szerveződésükre az adott földrajzi és politikai helyzet, a kriminális tradíció – mint az illegális igények – és a bűnüldözés felépítése, valamint annak hatékonysága.[6] A társadalmak Európa-szerte egyre inkább egymással összekapcsoltabbá, illetve nemzetközi jellegűvé váltak, ami ugyanígy a szervezett bűnözés működésére is jellemző, hogy összekapcsoltabbá és nemzetközileg aktívabbá vált mint valaha.

A szervezett bűnözői csoportok tevékenységi és működési köre („üzleti portfoliója") egyre változatosabb, bár a kábítószer-kereskedelem továbbra is a legjöve-

[4] Korinek László: A technika fejlődése és a bűnözés. In: Borbíró Andrea – Inzelt Éva – Kerezsi Klára – Lévay Miklós – Podoletz Léna (szerk.): A büntető hatalom korlátainak megtartása: A büntetés mint végső eszköz – Tanulmányok Gönczöl Katalin tiszteletére. ELTE Eötvös Kiadó. Budapest, 2014. 290. o.

[5] Tóth Mihály: A gazdasági bűnözés és bűncselekmények néhány aktuális kérdése. MTA Law Working Papers 2015/4. 5. o.: „A feketegazdaság – szűkebb, vagy tágabb értelemben – elsősorban a legális gazdasági szférán kívüli tevékenységre, a követhetetlenségre, ellenőrizhetetlenségre, (vagy konkrétabban az adózatlanságra) utal, és a gondok alapvető forrásának a láthatatlan jövedelmek képződését tartja."

[6] Tóth Mihály – Kőhalmi László: A szervezett bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016. 608. o.

delmezőbb tevékenységnek számít, azonban emellett jellemzően foglalkoznak még fegyverkereskedelemmel, embercsempészéssel, termékhamisításokkal és a kiberbűnözéssel is, és ezeket járulékosan a pénzmosás követi.[7]

A nagyobb „tradicionális", hierarchikus szervezett csoportok mellett a kisebb és lazább szerkezetű csoportok vannak jelen, amelyeket megbízott, speciális szaktudással rendelkező személyek erősítenek ad hoc jelleggel. Az is előfordul, hogy az egyes csoportok csak rövid időre alakulnak egy meghatározott illegális tevékenység elvégzéséig. Az Europol jelentése szerint jelenleg 5000 szervezett bűnözői csoport működik nemzetközi szinten, akikkel szemben folyamatban lévő nyomozás is van, míg 2013-ban csak 3600 ilyen csoportról számoltak be. A növekedés köszönhető a kisebb bűnözői csoportok megjelenésének, különösen az ún. bűnözői piacok (criminal market) népszerűségének, amelyeknek a működése és az alapjukat képező üzleti modell erősen függ az internettől. Ezen piacok fragmentáltsága különösen a kiberbűncselekményekkel kapcsolatban figyelhető meg, és ezeket növekvő számban önálló bűnelkövetők is mint egy vállalkozásként folytatnak, vagy akár többen együtt alkalmi jelleggel, hogy vállalkozásukat működtessék, ami általában illegális árucik-kekkel való kereskedést vagy különféle szolgáltatások nyújtását jelenti.[8]

Korinek László szerint – kriminológiai aspektusból vizsgálva – a szervezett bűnözést a következő ismérvek határozzák meg:

- a hatályos jogszabályok szerint tiltott szükségletek kielégítésére irányul,
- a lehető legkisebb kockázatvállalás mellett a leggyorsabb és lehető legnagyobb profitra törekvés jellemzi,
- a bűnözői csoportokon belül szakosodás, specializáció figyelhető meg,
- a szervezett bűnöző tevékenységét foglalkozásként űzi,
- jellemző az erőszak a bűnözőtársulás tevékenysége során,
- megfigyelhető a legális és illegális tevékenységek egyidejű jelenléte,
- a tevékenység nemzetközi, határokon átnyúló jellegű.[9]

2000 óta az Egyesült Nemzetek keretében létrejött nemzetközi szervezett bűnözés elleni Egyezmény határozza meg a nemzetközi fogalmát a szervezett bűnözői csoportnak, amely értelmében bizonyos ideig fennálló, három vagy több főből álló

[7] Abadinsky, Howard: Organized crime. Ninth Edition, Wadsworth Cengage Learning, 2010. 203. o.

[8] Europol: European Union Serious and Organised Crime Threat Assessment (SOCTA) – Crime in the age of technology. 2017. 14. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 [2018.03.21.]

[9] Korinek László: A szervezett bűnözés lényegi elemei. In: Harmadik Magyar Jogászgyűlés – Magyar Jogász Egylet. Budapest, 1996. 65-72. o.

strukturált csoportról[10] van szó, amely összehangoltan működik egy vagy több, az Egyezményben meghatározott súlyos bűncselekmény[11] elkövetése céljából, közvetlen vagy közvetett módon pénzügyi vagy más anyagi haszon megszerzésére törekedve.

Ezt a definíciót vette át az országok többsége, így Magyarország is. Ennek fényében a hatályos Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 459.§ (1) bekezdés 1. pontja határozza meg a bűnszervezet fogalmát, amely három vagy több személyből álló, hosszabb időre szervezett, összehangoltan működő csoport, amelynek célja ötévi vagy ezt meghaladó szabadságvesztéssel büntetendő szándékos bűncselekmények elkövetése.

Az említett bekezdés 2. pontjában foglalt értelmező rendelkezés a bűnszövetséget is definiálja, amely akkor létesül, ha két vagy több személy bűncselekményeket szervezetten követ el, vagy ebben megállapodik, és legalább egy bűncselekmény elkövetését megkísérlik, de nem jön létre bűnszervezet. E fogalomnak a negatív eleme, hogy nem jöhet létre bűnszervezet.[12]

Áttérve azonban a bűnszervezet fogalmi ismérveinek részletes vizsgálatára: az „összehangolt működés" tartalmát tekintve nem más, mint a benne cselekvő személyek egymást erősítő hatása. Ugyanakkor az összehangoltság meglétének – természetéből adódóan – nem feltétele a bűnszervezetben cselekvők közvetlen kapcsolata, a más cselekvések, illetve a más cselekvők kilétének konkrét ismerete. A bűnszervezetben elkövetés azzal szemben is megállapítható, aki – eseti jelleggel – akár egyetlen cselekményt tettesként vagy részesként valósít meg, tehát nem az alanyi bűnösség, hanem a bűnszervezet fogalmi elemei megállapításának kérdése a «hosszabb időre szervezett" kitétel, amely a több bűncselekmény rendszeres jellegű elkövetését jelenti, de a bűnszervezet oldalán. Az elkövető tudatának továbbá nem arra kell kiterjednie, hogy egy bűnszervezet a törvényi előfeltételek szerint létrejött, hanem arra, hogy a bűnszervezet tárgyi sajátosságai ismeretében annak „működéséhez" csatlakozik, illetve annak keretében cselekszik. A Btk. hatályos rendelkezései nem tesznek különbséget a bűnszervezeten belüli cselekvés hiearchiája („posztjai"), aktivitása, intenzitása szempontjából, ezek a büntetéskiszabás körében értékelendő

[10] A strukturált csoport nem egyetlen bűncselekmény azonnali végrehajtására, valamint nem alkalomszerűen létrehozott csoport. Nem szükséges, hogy tagjai pontosan meghatározott szerepekkel rendelkezzenek vagy, hogy tagsága állandó legyen, illetve hogy fejlett hierarchiával rendelkezzen.

[11] Az Egyezmény definiálja továbbá a súlyos bűncselekményt is, melynek értelmében legalább négy év szabadságvesztéssel vagy súlyosabb büntetéssel büntethető bűncselekményt megvalósító magatartást jelenti.

[12] Lásd bővebben Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017. 410-425. o.

körülmények.[13] A bűnszervezet megállapításához nem többletkövetelmény a bűnös profitszerzési célzat.[14]

A bűnszervezetben elkövetésre vont jogkövetkeztetésnek van helye – az egyéb törvényi feltételek megléte esetén –, ha az elkövetési magatartások egymást kiegészítő jellegűek, azok kapcsolódása a célzott és végrehajtott bűncselekményhez kölcsönös, az adott tényállásszerű elkövetési magatartás keretei közé illeszkedő cselekmény más személy előző cselekményéhez társul, avagy a célzott bűncselekmény megvalósulásához további láncolatos tevékenységet feltételez.[15] A bűnszervezet fogalmának utolsó objektív ismérve egy szervezeti célt határoz meg, amely szerint a bűnszervezet létének nem törvényi előfeltétele akár egyetlen bűncselekmény befejezett elkövetése vagy kísérlete sem. A Btk. nem sorolja fel, hogy milyen típusú bűncselekmények tartoznak ide csak annyit, hogy ötévi vagy ezt meghaladó szabadságvesztéssel büntetendő szándékos bűncselekményekről lehet szó. Ezzel kapcsolatban felmerül az a kérdés, hogy mindez azokra a bűnszervezetekre hogyan alkalmazható és miképpen minősíthető a szervezet működésébe becsatlakozó elkövetők magatartása, akik kihasználják az internet nyújtotta előnyöket és például az illegális tevékenységüket az online piacterekre kiterjesztve folytatják (pl. kábítószer-kereskedelem, gyermekpornográf tartalmak terjesztése stb.).

Mindezekre tekintettel azon az álláspontón vagyok, hogy amennyiben megvalósulnak a bűnszervezetnek a törvényi feltételei és az elkövető tudata át fogja azt, hogy bűnszervezethez kapcsolódva cselekszik – akár legyen szó csak egyszeri alkalomról –, akkor a bűnszervezetben történő elkövetés megállapítható, feltéve, ha az általa kapcsolódó bűncselekmény ötévi vagy súlyosabb szabadságvesztéssel büntetendő. Ugyanez vonatkozik a tetteseken kívül a részesekre is, tehát amennyiben a szükséges feltételek teljesülnek, akkor az esetükben is a bűnszervezetben elkövetésről van szó.[16] Ezt erősíti a Kúria friss eseti döntése is, amelyben kimondta, hogy a bűnszervezettel kapcsolatban elsődlegesen mindig a bűncselekmény elkövetését kell vizsgálni, majd az alanyi oldalt, az elkövető tudattartalmát, hogy felismerte-e, hogy az elkövetési magatartását a bűnszervezet keretén belül valósította meg. A törvény a bűnszervezet külső, tárgyi jellegű ismérveit határozza meg, ezért fontos, hogy ez a kívülálló számára is felismerhető legyen. A bűnszervezeten belüli személyes ismeretség valamennyi elkövetővel nem feltétele a megállapításának, és a bűnszervezet-

[13] 4/2005. számú BJE határozat; TÓTH Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009. 148-151. o.
[14] BH 2008. 139.
[15] BH 2018.4.106.
[16] BH 2010.11.472.

nek nem törvényi kritériuma a hierarchikus kapcsolat sem.[17] Hiszen a bűnszervezet létrejöhet úgyis, hogy a keretében bűncselekményeket irányító vagy vezető személy hangolja össze azoknak az elkövetőknek a magatartását, akik egymás tevékenységéről nem is tudnak.[18] Amennyiben mégis hierarchikus szervezetről van szó, akkor a bűnszervezet vezetője felbujtóként tartozik felelősséggel a bűnszervezet tagjai által elkövetett bűncselekményekért.[19]

Mindezt figyelembe véve a tudattartalom vizsgálatának körültekintően kell történnie, és ezzel párhuzamosan vizsgálni kell a büntetőeljárás során feltárt bizonyítási eszközökből származó, és a bűnszervezet fennállásának megállapításához szükséges ismérvekre következtetést megalapozó bizonyítékokat, és erre nézve a tényállásban megállapítást kell tenni.[20]

Amennyiben nem éri el a meghatározott büntethetőséget az elkövető cselekménye, akkor súlyosító körülményként értékelhető és nem alkalmazhatók a bűnszervezeti elkövetéshez kapcsolódó jogkövetkezmények. Más kérdés, ha például az elkövető cselekményei több részcselekményből tevődnek össze, ugyanakkor a természetes egységbe vagy a folytatólagosság egységébe olvadnak, és amely a szervezetbe tartozó tag esetében eléri az ötévi fenyegetettséget, akkor a joggyakorlat ebben az esetben megfontolandónak tartja annak megállapítását, hogy a bűnszervezet törvényi feltételei fennállnak. Azonban a szakirodalombam eltérő álláspont is található, mely szerint a bűnszervezeti elkövetés célja bűncselekmények elkövetése, a többes szám pedig egység-többségtani szempontból bűncselekményi többségre, egy eljárásban történő elbírálás esetén pedig bűnhalmazat fennállására enged következtetni. A nyelvtani értelmezés alapján a bűnszervezet hatókörének kiterjesztése aggályos lehet. Hasonlóan alakul a törvényi egység más esetkörei vagy a látszólagos halmazat esetén.[21]

Összességében elmondható, hogy a bűnszervezet fogalmába a bűnöző célzatú tartós struktúrák számos formája beilleszthető, amely alkalmas lehet arra, hogy egyrészről kifejezze az alkalmi kisebb súlyú bűnszövetséghez viszonyított többletkriminalitást, másrészről magában foglalja a szervezettség súlyosabb formájában rejlő veszélyességet is. A bűnszervezet keretében történő elkövetéshez bármely szándé-

[17] BH 2016.9.234.

[18] Csák Zsolt: Társas elkövetés, különös tekintettel a bűnszervezetre. In: Benisné Győrffy Ilona (szerk.): Negyvenegyedik Jogász Vándorgyűlés. Budapest, 2018. 328-329. o.

[19] EBH 2008.1849.

[20] BH 2014.131.

[21] ambrus István: Egység és halmazat – régi dogmatikai kérdés új megközelítésben. Szeged, SZTE ÁJK, 2014. 20. o.

kos bűncselekmény esetén súlyos általános részi jogkövetkezmények[22] társulnak – mivel a hatályos szabályok szerint általános jellegű minősítő körülmény –, míg a bűnszövetség esetében a bűncselekmény súlya közömbös, de csak akkor állapítható meg, ha a Különös Részben minősítő körülményként szerepel.[23]

A Btk. 321.§ (1) bekezdése szerint bűnszervezetben részvétel bűntette miatt büntetendő, aki bűncselekmény bűnszervezetben történő elkövetésére felhív, ajánlkozik, vállalkozik, a közös elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítja, illetve a bűnszervezet tevékenységét egyéb módon támogatja. A tényállás kétfajta elkövetési magatartástípust rendel büntetni: egyrészt sui generis előkészületi bűncselekményt, azzal, hogy bár eltérő sorrendben, de az előkészület fogalmát alkotó magatartásokat jelöl meg; másrészt sui generis bűnsegélyt azzal, hogy azt, aki – mint a bűnszervezeten kívülálló személy – a bűnszervezet tevékenységét támogatja büntetni rendeli. Az elkövetési magatartások a bűncselekmény bűnszervezetben történő elkövetéséhez kapcsolódnak és amennyiben, aki az előkészületi jellegű magatartását tovább folytatva saját maga is bekapcsolódik a szervezet tevékenységébe, és azt a magatartást, amelyre felhívott stb. megkísérli vagy annak megvalósításában tettesként közreműködik, értelemszerűen a bűnszervezetben elkövetett bűncselekmény tetteseként fog felelni. A Btk. Kommentárja azt rögzíti, hogy a bűnszervezet tevékenységének „egyéb módon támogatása" csak a szervezeten kívülálló személy részéről valósítható meg, és feltételezi a bűnszervezet létezését. E fordulat elkövetőinek a cselekménye nem közvetlenül a bűnszervezetben elkövetett bűncselekményhez, hanem magához a bűnszervezet működéséhez kapcsolódik és tisztában kell lenniük azzal, hogy

[22] Azzal szemben, aki a szándékos bűncselekményt bűnszervezetben követte el, a bűncselekmény büntetési tételének felső határa a kétszeresére emelkedik, de a huszonöt évet nem haladhatja meg. Halmazati büntetés esetén a 81. § (3) bekezdése szerinti büntetési tételt, tárgyalásról lemondás esetén a 83. § (1)–(2) bekezdése szerinti büntetési tételt kell alapul venni. [91. § (1) bek.];

Azzal szemben, aki a bűncselekményt bűnszervezetben követte el, mellékbüntetésként kitiltásnak is helye van. [91. § (2) bek.];

A kétévi vagy ennél hosszabb tartamú szabadságvesztést fegyházban kell végrehajtani [37. § (2) bek. bb) pont];

A feltételes szabadságra bocsátás kizárt [38. § (4) bek. c) pont];

A végleges hatályú foglalkozástól eltiltás alól a bíróság az eltiltottat nem mentesítheti, ha az eltiltás méltatlanság okán, véglegesen történt [Btk. 53. § (4) bek.];

A bűncselekmény eszközének és tárgyának elkobzása méltányosságból nem mellőzhető [73. § b) pont.];

A bűnszervezet ideje alatt szerzett vagyont az ellenkező bizonyításáig elkobzás alá eső vagyonnak kell tekinteni [74. § (4) bek. a) pont];

A büntetés végrehajtásának felfüggesztése kizárt [86. § (1) bek. b) pont];

A tevékeny megbánás (közvetítői eljárás) kizárt [29. § (3) bek. b) pont].

[23] Tóth Mihály: A bűnszervezeti elkövetés szabályozásának kanyargós útja. Magyar Jog 2015/1. 5-6. o.

akár anyagi vagy más természetű támogatással a súlyos bűncselekmények elkövetésére létrejött csoportosulás tevékenységét előmozdítják anélkül, hogy a bűnszervezetben elkövetett bármely bűncselekményhez segítséget nyújtanának.[24] Tóth Mihály vitathatónak tartja a lehetséges alanyok szűkítését, mert indokolatlanul privilegizált helyzetet teremt azoknak a csoport-tagoknak, akik a tudatos csatlakozáson kívül akár rendszeres finanszírozással vagy öt évet meg nem haladó büntethetőségű bűncselekményekkel támogatják a bűnös tevékenység előkészítését. Nem világos, hogy miért kellene a lehetséges alanyok körét tekintve különbséget tennünk pl. a bűncselekmény elkövetéséhez szükséges eszközök beszerzésében, rendelkezésre bocsátásában testet öltő magatartás és az anyagi eszközök rendelkezésre bocsátása, esetleg a tekintélyen, befolyáson alapuló pszichikai támogatás között.[25]

Ezzel szoros összefügésben érdemes arra kitérni, hogyha egy adott, kívülálló személyt (pl. informatikus szakembert) megbíznak az online bűnözői infrastruktúra kezelésére, annak biztosítására vagy egyéb tevékenységre (pl. rosszindulatú programok készítésére), ami kapcsolódik a szervezet működéséhez – sőt elősegíti azt –, akkor ez hogyan értékelhető. Amennyiben fennállnak a bűnszervezetnek a feltételei és az elkövető a folyamatosan végzett, de ötévi szabadságvesztéssel fenyegetettséget el nem érő cselekményei valós bűnszervezethez kapcsolódnak és ezek a súlyos bűncselekmények megvalósulását biztosítják, akkor a bűnszervezetben részvétel bűntettét valósítja meg.

A kiberbűncselekmények vonatkozásában fontos kiemelni a 2013/40/EU irányelvet az információs rendszerek elleni támadásokról, mert kimondja, hogy helyénvaló súlyosabb szankciókat megállapítani, ha az információs rendszer elleni támadást bűnszervezetben követik el, valamint, ha jelentős számú információs rendszert érint.[26]

3. A kiberbűnözői csoportok tipológiája

A kiberbűnözői csoportok tipológiáját átfogóan Michael McGuire vizsgálta, aki a kutatása során az általa feltárt ügyek alapján arra a következtetésre jutott, hogy az informatikai bűnözéssel kapcsolatos esetek 80%-a valamilyen szervezett tevé-

[24] Belegi József: A közbiztonság elleni bűncselekmények – Btk. XXX. fejezet. In: Kónya István (szerk.): Magyar büntetőjog I-III. – új Btk. – Kommentár a gyakorlat számára. 5. kiadás, HVG Orac Lapkiadó Kft. 2016.

[25] Tóth (2015): i.m. 7. o.

[26] Nagy Zoltán András: A 2013/40-es Uniós direktíva az informatikai rendszereket érő támadásokról. http://www.rendeszetelmelet.hu/Graphics/pdf/Nagy_Zoltan_Andras_A_2013_40_es_Unios_direktiva.pdf [2018.02.28.]

kenység eredménye. Ez azonban nem jelenti azt, hogy az elkövetők a tradicionális és hierarchikus szervezett bűnözői csoportokhoz tartoznának vagy kizárólag kiberbűncselekményeket követnének el. A tanulmányában arra hívja fel a figyelmet, hogy a hagyományos bűnszervezetek egyre inkább kiterjesztik a tevékenységüket az interneten, emellett újabb és kevésbé szoros kapcsolatú bűnözői csoportok jelennek meg. A bűnözői csoportok különböző szintű szervezettséget mutatnak, attól függően, hogy a tevékenységüket csak online fejtik ki, vagy online eszközöket használnak, hogy lehetővé tegyék a bűncselekmények elkövetését a „való" világban, vagy ezek kombinációja jelenik meg online és offline is.

McGuire egy tipológiát ajánl a kiberbűnözői csoportokkal kapcsolatban, amely hatféle csoport felépítését foglalja magában, kihangsúlyozva, hogy ezek az alapvető szervezeti minták gyakran keresztezik egymást és rendkívül rugalmasan alakulhatnak akár megtévesztő módon. Felhívja a figyelmet arra is, hogy mindez a folyamatos technológiai fejlődésnek köszönhetően változni fog a jövőben. Három főcsoportot különböztet meg, amelyeket további két alcsoportokra bont a tagok között fennálló kapcsolat erőssége alapján. Az első főcsoport online működik és további két alcsoportra osztható, amelyek a következők: a „swarm" és a „hub".

A „swarm" egy olyan csoport, amely valamely közös cél érdekében tevékenykedik, irányítás és szervezett működés nélkül. Általában az ideológiai vagy politikai indíttatású csoportok tartoznak ide, amelyek online fejtik ki a tevékenységüket mint például ilyen az Anonymous hacktivista csoport is.

A „hub" csoportok szintén online működnek, de a „swarm"-hoz képest szervezettebbek és hierarchikusabbaknak tekinthetők, mert meghatározott „irányító, létrehozó" kulcstagok köré csoportosulnak „az egyszerű" tagok. A tevékenységük széleskörű magában foglalhatja az ún. „crimeware"[27] terjesztést, az adathalász támadásokat (phishing) és a gyermekpornográfiát. McGuire szerint az online feketepiacok működése illeszkedik ebbe a modellbe.

A második főcsoportba tartoznak azok a hibrid csoportok, amelyek online és offline is jelen vannak.

A „clustered hybrid" esetében egy kisszámú csoportról van szó, amely meghatározott és speciális tevékenységgel foglalkozik. A „hub" felépítéséhez hasonló, de a különbség az, hogy az online elkövetés mellett az offline is megjelenik például bankkártyákat skimmelnek majd az interneten árulják a megszerzett bankkártya adatokat.

[27] A crimeware olyan rosszindulatú programokat foglal magában, amikkel az elkövetők célja, hogy haszonra tegyenek szert és egyúttal a felhasználók pénzügyi jólétét vagy értékes adatait veszélyeztessék (pl. a vírusok, a trójai vagy keylogger, amik a bűnözői csoportok számára lehetőséget teremtenek az adatok ellopásához, illetve azokkal való kereskedéshez).

Az „extended hybrid" csoportok kevésbé centralizáltak, általában többen társulnak és kisebb alcsoportokra osztható, de a különféle bűncselekmények elkövetéséhez megfelelő koordinációval rendelkeznek.

A harmadik főcsoport azokat a csoportokat foglalja magában, akik elsősorban offline fejtik ki a tevékenységüket, de egyúttal a modern technológiák és az internet nyújtotta előnyöket is kihasználják már.

A „hierarchies" azok a tradicionális bűnözői csoportok, akik illegális tevékenységüket az interneten is kifejtik, ilyenek lehetnek a tradicionális maffia családok, akik például a prostitúcióhoz kapcsolódó tevékenységüket kiterjesztik a pornográf, különösen a gyermekpornográf weboldalakra, illetve online szerencsejáték oldalakat üzemeltetnek vagy a zsarolást kibertámadások felhasználásával követik el.[28] A nemzetközi szindikátusok is érintettek a kiberbűnözésben mint például a Triádok vagy Yakuzák, akik szoftver kalózkodással, bankkártya hamisításokkal és csalásokkal is foglalkoznak.[29]

Az „aggregate" csoportok pedig lazán szervezettek, ad hoc jelleggel működnek. Például mobiltelefonokat használnak a csoport tevékenységének a koordinálásához vagy a nyilvános zavargás szervezéséhez.[30]

A téma szempontjából két csoportot érdemes kiemelni és részletesen ezek összehasonlításával foglalkozik a szerző: a „hierarchies", a tradicionális szervezett bűnözői csoportok és a „hub" mint az új típusú kiberbűnözői csoport.

4. A tradicionális szervezett bűnözői csoportok és a kiberbűnözői csoportok összehasonlítása

A tradicionális szervezett bűnözői csoportok általában etnikailag homogének, és hierarchikusan strukturáltak, valamint multifunkcionális és bürokratikus szervezeteknek tekinthetők. Az összehasonlítás alapját képező másik új típusú csoportosulás pedig az ún. „szervezett" kiberbűnözői csoport, amelynek meghatározására Marie-Helen Malas tett kísérletet: egy strukturált csoport, amely három vagy több tagból áll, amelynek célja egy vagy több súlyos kiberbűncselekmény anyagi haszonszerzési célú elkövetése az információs rendszerek, az internet felhasználásával.[31]

[28] McGuire, Michael: Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security. 2012.

[29] Kim-wang, Raymond – Choo-Grabosky, Peter: Cybercrime. In: Paoli, Letizia: The Oxford Handbook of Organized Crime. Oxford University Press, 2014. 485. o.

[30] Broadhurst – Grabosky – Alazab-Chon: i.m. 7. o.

[31] Malas, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017. 365 o.

A kiberbűnözői csoportok fejlődésük során soha nem mentek végbe olyan szintű szervezettségen mint a hagyományos bűnszervezetek. Az egyéni és fragmentált bűnözői tevékenységek felől mozdultak el a modern vállalati üzleti modellek alkalmazása felé és általában a hierarchikus felépítés hiányzik belőlük. A rugalmas kapcsolatrendszer jellemző rájuk, tagjaik magasan képzett szakemberek és általában a speciális szakismeretüknek, tudásuknak megfelelő feladatot látnak el, amivel hozzájárulnak a különféle crimeware és azokhoz kapcsolódó szolgáltatások fejlesztéséhez.

Míg a tradicionális bűnszervezetek ismérve, hogy erőszakos módon törekednek arra, hogy fenntartsák a monopol helyzetüket a saját területük, illetve érdekeltségük alá vont javak felett annak érdekében, hogy ellenőrzésük alatt tarthassák az általuk dominált piacot, addig a területi kontroll az interneten nyilván nem kivitelezhető a virtuális környezet sajátosságaiból adódóan, éppen ezért kedvező feltételeket biztosít azok számára is, akik amúgy az adott piacról kiszorulnának. Továbbá a kontroll mechanizmus még nehezebbé vált, mert a tagok között nincs szükség személyes kapcsolattartásra – sőt általában kizárólag elektronikus csatornákon keresztül kommunikálnak egymással – és a csoport működéséhez nem kellenek a formális szervezeti keretek (pl. a klasszikus hierarchikus szervezeti struktúra nem megfelelő a kiberbűnelkövetők számára). Az új típusú szervezett bűnözés működése a digitális környezetben hasonlóságot mutat a modern vállalati világhoz különösen, ami az alkalmazott árazási stratégiát, szolgáltatás-alapú versenyt, innovációt és az „ügyfélszolgálatot" illeti. A kiberbűnözői csoportok ereje a rendelkezésre álló szoftver fejlettségben rejlik és nem a csoport tagjainak a számában. Az alkalmazott automatizált műveletek nem csak a bűncselekmények elkövetéséhez és az online feketepiacok létrejöttéhez járultak hozzá, hanem a szervezeti struktúrára nézve is meghatározó tényezővé váltak, mert az emberek helyett a technológia került a középpontba.

A kiberbűnözőkre jellemző, hogy egyre nagyobb mértékben veszik át és másolják a legális vállalatok üzleti modelljeit, a 2000-es évek óta fejlesztenek ki olyan üzleti mintákat, amelyek az eBay, Yahoo, Google és az Amazon high-tech cégek által használtakhoz hasonló. A „kiberbűnözői iparágat" már a professzionalitás és kifinomultság határozza meg a különféle kibertámadások terén, illetve a specializáció vagyis munkamegosztás az elkövetők között, a kommercializáció és az integráció, ami azt jelenti, hogy az egyes jogsértéseket további jogsértés követi mint például az adatlopást követően eladható a megszerzett adat, majd azt csalásra használhatják fel.

Az vitatott, hogy az informatikai bűnözés által megteremtett üzleti modell és a legálisan működő vállalkozások között milyen eltérések mutatkoznak: míg utóbbi a vásárlók számára az értékteremtést célozza, addig a kiberbűnözés magában foglalja az áldozatok kijátszását a kreatív csalások révén és a kockázat minimalizálását arra vonatkozóan, hogy az illegális tevékenységüket elfedjék. Azonban, ha az informati-

kai bűnözést olyan modellnek tekintjük, ami kapcsolatot teremt az illegális eszközök, szolgáltatások „beszállítója" és a vásárlók között, akik ezeket bűncselekmények elkövetésére használják fel az áldozatokkal szemben, akkor ez a különbség nem jelentős, hiszen ez a rendszer is arra összpontosul, hogy értéket teremtsen a „fogyasztói" részére, akik azonban jelen esetben a kiberbűncselekmények elkövetői lesznek.

Az innováció eredményeképpen, a bűnözői ökoszisztémában új minták jelentek meg – amit mindkettő csoport ki is használ – mint például az áruk elhelyezésével, alvállalkozásokkal és kapcsolatépítéssel kapcsolatban. Olyan üzleti modellt alkalmaznak (Criminal-to-Criminal), amely hasonlóságot mutat a jogszerűen működő vállalkozásokéhoz (Business-to-Business), azonban ennek középpontjában az egymás közötti illegális áruk adásvétele és a tiltott szolgáltatások nyújtása áll az informatikai hálózatokon keresztül.[32]

Az automatizáció jelentős szerepet játszik a C2C modellek fejlődésében, mert idő- és költséghatékonyabbá teszi a működésüket. Az automatizált bűnözői tevékenységek alapját a botnet hálózatok képezik, amelyek a felhasználók tudta nélkül megfertőzött számítógépekből állnak és ezek az elkövetők által távolról irányíthatók mint egy „zombigépként". A használatuk révén akár nagyszabású támadásokat indíthatnak (pl. DDoS támadást[33]), különböző rosszindulatú programokat tudnak terjeszteni, vagy nagy mennyiségű személyes, illetve egyéb bizalmas adatokhoz is hozzájuthatnak a spamküldések és az adathalász technikák alkalmazásával.[34]

5. Specializáció és munkamegosztás

A kiberbűnözői iparág széleskörű tevékenységi kört ölelhet fel, amelyben az elkövetők funkcionálisan specializálódnak az egyes feladatokra, tehát jelen van munkamegosztás és ez a következőképpen alakulhat:

A programozók azok, akik a különböző rosszindulatú programokat (malware) írják meg és egyéb eszközöket rendelkezésre bocsátják, amelyek a bűncselekmények elkövetéséhez szükségesek.

[32] Tropina, Tatiana: The evolving structure of online criminality. eucrim 2012/4. 160-162. o.

[33] A DDoS támadás (Distributed Denial of Service) vagy másnéven szolgáltatásmegtagadással járó támadás egy olyan támadási forma, amelynek a célja az információs rendszerek, szolgáltatások vagy hálózatok erőforrásainak oly mértékben történő túlterhelése, hogy azok elérhetetlenné váljanak, vagy ne tudják ellátni az alapfeladatukat. Az ilyen elektronikus támadást intézők a jogosult felhasználókat akadályozzák a szolgáltatás igénybevételében. Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009. 115.o. http://www.cert-hungary.hu/ddos [2018.03.05.]

[34] Tropina: i.m. 160. o.

A forgalmazók vagy eladók, akik kereskednek és eladják a lopott adatokat és szavatolják az árukat, amiket mások biztosítanak a számukra.

A technikusok, akik fenntartják a bűnözői infrastruktúrát, a technológiai támogatást biztosítják mint például a szerverek és a titkosítás zavartalan működését. A gazdagép (host), az a hálózatra csatlakoztatott számítógép, amely az illegális tartalmakat biztosító szervereket és hálózatokat kezeli sokszor botnetek és proxy hálózatok révén.

A hackerek, akik a sebezhetőségeket keresik a rendszerekben, programokban, illetve hálózatokban azzal a céllal, hogy rendszergazda szintű jogosultságot vagy ún. „root level access", illetve „god level access" szintű hozzáférést szerezzenek.

A csalás specialisták pedig különböző ún. social engineering[35] sémát dolgoznak ki és alkalmazzák azokat mint például a phishing és a spam küldés is ilyen.

A „pénztárosok" kezelik a bűnös eredetű pénzt és a hozzá tartozó fiókokat, és más bűnözők számára is biztosítják ezeket megfelelő díjazás fejében, továbbá általában ők felügyelik az önálló pénzfutárok, ún. „money mule"-ok tevékenységét is.

A pénzfutárok segítenek a bűncselekményekből befolyt bevételeknek az átutalásában harmadik félnek, hogy az további utalással biztonságosan elhelyezze a pénzt. Vannak olyan személyek, akik az átutalásokért és a pénz tisztára mosásáért felelnek digitális valuták és különböző országok pénznemei közötti átváltásokkal.

Végül a végrehajtók azok, akik kiválasztják a célpontokat, toboroznak és kijelölik a tagokat az említett feladatokra, ezen felül pedig a bűncselekményekből származó bevételek elosztásáért felelnek.[36]

6. Az online feketepiacok és fórumok

A kiberbűnözés egy profit-orientált, szolgáltatás-alapú üzleti modellé (Crime-as-a-Service) nőtte ki magát, amely által elérhetővé váltak olyan szolgáltatások a Surface Weben[37] vagy a Darkneten[38], melyekkel bármilyen kiberbűncselekmény elkövet-

[35] Mitnick, Kevin D.: A megtévesztés művészete című könyvnek a borítója: „A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."

[36] Chabinsky, Steven R. (2010): https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom [2018.03.05.]

[37] A hagyományos böngészők használatával szabadon elérhető része az internetnek.

[38] A Darknet egy elosztott, anonimitást biztosító, titkosított hálózat a Deep Weben belül, ami kizárólag speciális szoftverek használatával érhető el mint például a The Onion Routerrel (TOR), I2P-vel vagy Freenettel, amelyek magasfokú titkosítással vannak ellátva. A bűnelkövetők kihasználják ezeket, mert a használatuk révén könnyedén eltudják rejteni a személyazonosságukat, az internetes forgalmukat és a szerverük helyét.

hető. Ahogy már korábban említésre került ezt az üzleti modellt az önálló kiberbűnözőktől kezdve – akik számára az internet lehetővé teszi a szervezeti kerethez kötöttség nélküli tevékenység végzését – a szervezett kiberbűnözői üzleti társulások vagy akár a tradicionális szervezett bűnözői csoportok is alkalmazhatják. Utóbbiak, amennyiben nem rendelkeznek a szükséges technikai ismeretekkel és eszközökkel, akkor ők is megtudják vásárolni a fórumokon keresztül, akár a kiberbűnözőktől.

A különböző illegális online tevékenységek egy egyre fejlettebb és önálló digitális feketegazdaságot hoztak létre, amelyen belül speciális weboldalakat üzemelnek, ún. online feketepiactereket és fórumokat, amelyeket arra használnak, hogy a tilalmazott árukkal kereskedjenek és szolgáltatásokat hirdessenek, amiket együttesen „hidden services"-nek, azaz rejtett szolgáltatásoknak hívnak.

A piactereken és fórumokon belül gyakran jelen van egy merev és egyedülálló struktúra, ami a kijelölt szerepekkel, feladatmegosztással és az eltérő felelősséggel lehetővé teszi, hogy a tagok hatékonyan biztosítsák a fórum működésének a rendjét. Ezeket a fórumokat az adminisztrátorok irányítják, akik meghatározzák az adott fórum célját és a működéshez szükséges szabályokat. Az alfórumokat pedig moderátorok ellenőrzik, akik megbízható személyek, gyakran az alfórum témájában jártas szakemberek és ezért annak a tartalmát kezelik. A fórumokon találhatók nagyszámú eladók is, akik különféle szolgáltatásokat nyújtanak és a termékekkel kereskednek a fórum tagjaival. Az eladói státusz eléréséhez általában próbamintát kell a moderátorok számára nyújtani, akik értékelik azt, majd később a szolgáltatás vagy termék további folyamatos értékelést és pontozást kap a vásárlóktól. Az értékelést és visszajelzést biztosító rendszer hasonló a legális kereskedelmi oldalakéhoz azzal a kivétellel, hogy a bűnözők számára a magas értékelés, vagyis „a jó hírnév" elérése nem olyan egyszerű. Lényegében ezek az online fórumok biztosítják a szükséges logisztikát a felhasználók számára, hogy különféle kiberbűncselekmény elkövetésében részt vehessenek a megszerzett ismeretek és eszközök révén.[39]

Az illegális árukkal való kereskedésnek a Darkneten keresztül számos előnye van mind az eladók és mind a vásárlók részéről is. A Peer-to-Peer (P2P) technológiára épülő platformoknak köszönhetően az eladók és a vásárlók is közvetlenül kapcsolatba tudnak lépni egymással és közvetítő nélkül tranzakciókat folytathatnak le. Ezeket magasfokú anonimitás jellemez, amely során egyik félnek sem kell személyes adatot megadnia, bár a vásárló számára a fizikai áruk vásárlásakor nyilván meg kell adni egy szállítási címet, azonban manapság a kézbesítés különböző anonim he-

[39] Europol: The Internet Organised Crime Assessment (IOCTA) 2014. 19-21. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014 [2018.03.25.]

lyekre is történhet (pl. csomag automatákba), így az áruk átvételekor is biztosítható az áruért érkező személy anonimitása. A tranzakciók lebonyolításához nehezen lenyomozható ún. virtuális fizetőeszközöket használnak mint például ilyen a Bitcoin és az egyéb altcoinok (pl. Etherum, Zcash, Monero). Használatuk népszerű, mert pszeudoanonimitást biztosítanak, ami azt jelenti, hogy az utalások végrehajtásához nincs szükség azonosításra, illetve hitelesítésre, ezáltal azok nem köthetők konkrét személyekhez. További előnyként említhető, hogy decentralizáltak, vagyis központi felügyeleti szerv nélkül működnek, tehát nem tartoznak egy jegybankhoz vagy országhoz sem, ami a nyomozást tovább nehezíti, mert a nyomozó hatóságok nem tudnak kihez fordulni mint mondjuk egy pénzintézet esetén. A kriptovaluták kihívást jelentenek, mert nincs egységes jogi szabályázásuk és országonként eltérő a megítélésük: kérdéses, hogy pénznek, árunak vagy vagyoni értékű jognak tekinthetők-e. Általában fizetőeszközként funkcionálnak, amikor használatuk az illegális tevékenységekhez kapcsolódik, valamint pénzmosási és terrorizmusfinanszírozási kockázatot jelentenek.[40] Külön érdekesség, hogy a büntetőeljárásról szóló új 2017. évi XC. törvény már külön nevesíti az elektronikus adatot a bizonyítási eszközök között.[41] A 315. §-ban pedig kialakította az ún. virtuális vagyontárgyak biztosításának a keretszabályait, amely alapján a virtuális fizetőeszközök mint a Bitcoin, valamint az elektronikus pénz egyes típusai is a jövőben lefoglalás tárgyát képezhetik.[42]

Az online feketepiacokon, illetve fórumokon jellemzően az alábbi áruk adásvétele zajlik: kábítószer, gyermekpornográf tartalmak, hamis és hamisított áruk, fegyverek és crimeware.

6.1. Kábítószer-kereskedelem

A kábítószer-kereskedelem továbbra is a legnagyobb illegális piacnak számít és egyre több hagyományos szervezett bűnözői csoport vesz részt a különféle kábítószer előállításban, forgalmazásban és terjesztésben, amely során az internet nyújtotta előnyöket is kihasználják. A különböző feketepiacok fő profilját is a kábítószer adja mint például ilyen híres online „bazár" volt a Silk Road és az Alphabay is. Az egyes tanulmányok szerint a havi bevétele az első nyolc Darknet piactérnek 10,6 millió és 18,7 millió euró között mozog, amely kizárólag a kábítószer-kereskedelemből szár-

[40] Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/11. 639-647. o. https://fintechzone.hu/rendvedelmi-szervek-latokoreben-a-kriptovalutak/ [2018.04.30.]

[41] Lásd a digitális adatokról Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8. 441-442. o.

[42] Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2. 126. o.

mazik.[43] A kábítószer-kereskedelmet a Btk. 176.§-ban szabályozza, mely szerint, aki kábítószert kínál, átad, forgalomba hoz, vagy azzal kereskedik, bűntett miatt két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.

A kábítószer-kereskedelmen (Btk. 176.§) kívül szóba jöhetnek még a hazai szabályozás értelmében a következő bűncselekmények, amelyek a tiltott szerekhez kapcsolódnak: a kábítószer készítésének elősegítése (Btk. 182.§), kábítószer-prekurzorral visszaélés (Btk. 183.§), új pszichoaktív anyaggal visszaélés (Btk. 184.§), teljesítményfokozó szerrel visszaélés (Btk. 185.§), valamint a gyógyszerhamisítás (Btk. 185/A.§).

6.2. Gyermekpornográfia

A gyermekpornográf tartalmak készítése, illetve azzal való kereskedés jövedelmező üzletté vált, amit a szervezett bűnözői csoportok is felismertek és kihasználnak. A Darkneten keresztül hirdetik és terjesztik a tiltott pornográf tartalmakat vagy külön weboldalakat hoznak létre haszonszerzési céllal. Új trendként jelent meg, hogy a gyermekmolesztálást az interneten keresztül élőben közvetítik, vagyis „streamelik". Az online tevékenység célja egyben lehet az offline szexturizmus iránti igény felkeltése is. A Btk. 204.§ (1) bekezdés a)-c) pontja értelmében, aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt megszerez vagy tart, készít, kínál, átad vagy hozzáférhetővé tesz, forgalomba hoz, azzal kereskedik, illetve ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tesz az gyermekpornográfia bűntette miatt két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.

6.3. Hamis és hamisított termékekkel kereskedés

Az Europol szerint a hamis és hamisított termékek is népszerűek, amelyek széles skálája elérhető mind a Surface Weben és a Darkneten is: ruházati termékek, ékszerek, „kalóz" szoftverek, gyógyszerkészítmények, előfizetések különböző TV és zenei platformokhoz, online játék fiókokhoz, valamint a legkeresettebb termékek közé tartoznak a hamis pénzek és személyazonosító okmányok.

6.4. Crime-as-a-Service üzleti modell

A Crime-as-a-Service üzleti modellt követve az online feketepiacokon különböző szolgáltatások érhetők el, így a következők:

[43] Europol (2017): i.m. 49-50. o.

Infrastruktúra mint szolgáltatás (Infrastructure-as-a-Service): az informatikai támadások végrehajtásához szükség van egy védett infrastruktúrára, ami biztosítja a biztonságot, anonimitást és ellenállást a bűnüldöző hatóságok beavatkozásai elől. A tárhelyszolgáltatók (hosting providers), különösen az ún. „bulletproof hosting" szolgáltatások népszerűek, mert lehetőséget biztosítanak arra, hogy a felhasználók szabadon feltöltsék a kívánt tartalmat anélkül, hogy azokat eltávolítanák, még akkor is, ha illegálisnak minősülnek. Éppen ezért kulcsfontosságú szerepük van az online feketepiacok esetében, mert biztonságos tárhelyet biztosítanak a crimeware-nak, az ellopott adatoknak és egyéb illegális tartalmaknak. A VPN, vagyis a virtuális magánhálózat és a proxy szolgáltatások pedig fontos szerepet játszanak az anonimitás biztosításában, ezáltal segítenek a bűnüldöző szervek kijátszásában.

Az adat a legkeresettebb áru manapság. Nagy mennyiségű személyes és pénzügyi adatok adásvétele zajlik a digitális feketegazdaságban.[44] Az adat befolyásolja az illegális piacok fejlődését: meghatározott bűnözői tevékenységeket fejlesztettek ki, illetve folyamatosan dolgoznak azon, hogy javítsák, jobbá tegyék ezeket, annak érdekében, hogy hatékonyan szerezzék, „lopják el" ezeket az érzékeny adatokat (pl. phishing, malware és egyéb eszközök használatával a kereskedelmi, pénzügyi adatbázisokkal szembeni támadásokhoz).[45] A bankkártya és bankfiók adatokon kívül elérhetőek lakcímek, telefonszámok, e-mail címek, e-pénztárcák, társadalombiztosítási azonosítók és egyéb online felhasználó fiókokhoz kapcsolható adatok, különösen, amelyekhez pénzmozgás köthető.

Pay-per-install szolgáltatások népszerű módszerei a malware terjesztésnek, ami úgy működik, hogy akik a szolgáltatást nyújtják, azok terjesztik a rosszindulatú fájlokat, amiket pedig a szolgáltatást igénybe vevők biztosítanak a számukra és a letöltések száma utána fizetnek nekik. Az ilyen szolgáltatások országspecifikus forgalmat biztosíthatnak. További népszerű szolgáltatás, hogy a DDoS támadások indítására szolgáló botneteket, illetve a létrehozásukra szolgáló eszközöket, programokat lehet igénybe venni (DDoS-for-hire vagy DDoS-as-a-Service) – napi vagy havi díjjal átlagosan 5$ és 1000$ közötti áron.[46] Hasonlóképpen a különböző rosszindulatú programokhoz (pl. vírusokhoz) is hozzá lehet jutni szolgáltatásként mint például a legkönnyebb pénzszerzési módhoz: a zsarolóvírushoz (Ransomware-as-a-Service). A legnagyobb veszélyt pedig az egyedi hatású és célzott támadásokra kifejlesztett kártékony programok jelentik különösen, amelyek a kritikus infrastruktúrákat célozzák és ezek is már elérhetőek a feketepiacokon (pl. a Stuxnet ismertté válásával

[44] Europol (2014): i.m. 19-21. o.
[45] Tropina: i.m. 162. o.
[46] Europol: (2014): i.m. 19-21. o.

„közkinccsé vált", ezután annak elemei kikerültek a „szabadpiacra" és tovább fejlesztve már hasonló mechanizmusokat tartalmazó malware-ek is elérhetővé váltak mint a DuQu).[47]

Azért különösen veszélyes a Criminal-as-a-Service üzleti modell, mert könnyen hozzá lehet jutni a kiberbűncselekmények elkövetéséhez szükséges ismeretekhez, programokhoz, akár kész bűnözői infrastruktúrához, és ezért is fontos, hogy már az előkészületi cselekmények sui generis bűncselekményként kerüljenek meghatározásra. Hiszen a szolgáltatás igénybevételével a hozzá nem értő felhasználók is olcsón, egyszerűen és gyorsan tudnak támadást indítani, sokszor csak egy egérkattintás az egész, sőt a végrehajtáshoz még technikai segítséget is kapnak. Ennek megfelelően a Btk. 424.§-ban szabályozza az információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétségét, melynek értelmében büntetendő, aki a Btk. 375.§ szerinti információs rendszer felhasználásával elkövetett csalás, a 422.§ (1) bekezdés d) pontjában szabályozott tiltott adatszerzés vagy a 423.§-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez vagy forgalomba hoz; valamint aki, a jelszó vagy számítástechnikai program készítésére vonatkozó szervezési ismeretet más részére rendelkezésére bocsát. A megszerzett ismeretekkel kiberbűncselekményeket tudnak elkövetni, amit a Btk. a 423.§-ban az információs rendszer vagy adat megsértése bűncselekmény körében szabályozza a jogosulatlan vagy jogosultság keretének túllépésével elkövetett módozatokat, így az (1) bekezdés a jogosulatlan belépést (ún. hacking), (2) bekezdés a) pontjában az információs rendszer akadályozását (pl. DDoS támadás), valamint a b) pontjában az adat megváltoztatását, törlését vagy hozzáférhetetlenné tételét, végül a (3) és (4) bekezdés szerinti minősített esetek valósulnak meg, ha jelentős számú információs rendszert (pl. botnet alkalmazása), illetve közérdekű üzemet érint a bűncselekmény.

Hacking mint szolgáltatás (Hacking-as-a-Service): Alap szinten ez magában foglalhatja az e-mail vagy közösségi oldalak fiókjainak a feltörését vagy összetettebb támadásokat mint a gazdasági kémkedés vagy személyes adatok gyűjtését a meghatározott célponttól.

Fordításokhoz kapcsolódó szolgáltatások: A támadások sokszor országspecifikusak és előfordulhat, hogy az elkövető nem feltétlenül beszéli a célország nyelvét, ezért igénybe vehet szolgáltatást fordítóktól, akik helyesen megfogalmazott szöve-

[47] Nagy Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula-Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIII. 2012. 227-228. o.

geket nyújtanak nekik, ezzel maximalizálva a támadás sikerét, mert sok esetben éppen a nyelvtani pontatlanságok lehetnek árulkodó jelei a csalásnak.

Pénzmosás mint szolgáltatás (Money laundering-as-a-Service): A bűnözők nem csak saját maguk javára végeznek pénzmosást, hanem szolgáltatásként is elérhető általuk az meghatározott díj ellenében.[48] Azért, hogy „tiszta" profitra tegyenek szert az illegális tevékenységükből a „piszkos pénzek" tisztára mosásához különféle szolgáltatásokat vehetnek igénybe annak érdekében, hogy ezeket a legális gazdaságba vissza tudják forgatni.[49] Ezek a szolgáltatások magukban foglalják az online és offline megoldások kombinációit, amelyeknek a középpontjában általában a pénzfutárok hálózatok állnak. A „money mule" elnevezéssel ismert új pénzmosási technika a pénzintézetekkel történő kapcsolatfelvételt iktatja ki és egy harmadik személy – azaz a pénzhordó személy – közreműködésével terítik, bújtatják a bűncselekményből eredő „piszkos pénzt". Az elkövetők munkaszerződést ajánlanak a pénzfutárnak, amelynek keretében a megkeresett fél „munkája" annyi lenne, hogy saját bankszámláján jelentősebb összegeket kell fogadnia, majd azt készpénzben felvenni, vagy a „munkáltató" által megadott számlákra továbbutalni magas jutalékért cserébe. Indokolt tehát a fokozott óvatosság, hiszen aki akár az igen vonzónak tűnő ajánlatot elfogadja, maga is érintetté válik a pénzmosás bűncselekmény elkövetésében.[50] A pénzmosásnak (Btk. 399.§) a három fázisa, így az elhelyezés, rétegzés és az integráció ezekben az esetekben is megvalósul. Ezzel szoros összefügésben új trendként jelent meg, hogy a nagyobb összegek tisztára mosása úgy történik, hogy azt kisebb összegű tranzakciókra bontják (micro money laundering), melynek előnye, hogy kevésbé feltűnő, mert a sok kicsi sokra megy elvet követi.[51]

7. Egyéb illegális tevékenységek

7.1. Online szerencsejáték

A hagyományos szervezett bűnözői csoportok számára népszerű bevételi forrást jelentenek az általuk üzemeltetett különböző online szerencsejáték oldalak is, amelyek alkalmasak az illegális bevételek tisztára mosására. A virtuális hálózatokon is,

[48] Europol (2014): i.m. 19-21. o.

[49] Tóth Mihály: Gazdasági bűnözés és bűncselekmények. KJK-KERSZÖV Jogi és Üzleti Kiadó Kft. Budapest, 2002. 375. o.

[50] Europol (2014): i.m. 19-21. o.; Kármán Gabriella – Mészáros Ádám – Tilki Katalin: Pénzmosás a gyakorlatban. Ügyészségi Szemle 2016/3. 88. o.

[51] Maras: i.m. 336. o.

akár a valós térben elterjedtek a különféle szerencsejátékok és fogadási oldalak. Általában az ismeretlen felhasználókkal korrektnek nevezhető módon játszanak, de a „bennfentes" felhasználók csak vesztenek, azaz csak befizetnek oda.[52]

7.2. A zsarolás új formái

A DDoS támadásokat zsarolási céllal is felhasználják, amely során olyan cégek oldalait választják ki, amelyek folyamatos és zavartalan működést követelnek meg (pl. webshopok, online szerencsejáték és fogadó cégek, energia- és pénzügyi szféra) és ezekkel szemben kisebb támadást indítanak, és a további erőteljesebb – akár teljes rendszer leállást eredményező – támadások elkerülése érdekében Bitcoint kérnek fizetségért. 2016-ban az Europol sikeres akciót hajtott végre és letartóztatta a zsarolásokban élen járó DD4BC (Distributed Denial of Service for Bitcoin) Team hacker csoportnak a kulcsfontosságú tagjait, akik számos DDoS támadást indítottak szervezetten európai cégekkel szemben.[53] Ezen kívül a túlterheléses támadással történő zsarolás a terroristák fegyvertárába is tartozik.[54]

Europol továbbá figyelmeztet a zsarolás új formájára, amikor a kiszemelt sértettektől kompromittáló képfelvételeket szereznek meg például a közösségi médián keresztül a bizalmukba férkőzve majd a felvételek megosztásával fenyegetnek, amennyiben meghatározott összeget Bitcoinban nem fizetnek. Ezek az esetek egyre növekvő számban bűnszervezetekhez köthetők, akik mint egy „call center"-t működtetnek haszonszerzési céllal.[55]

8. Összefoglalás

A bűnelkövetők gyorsan átveszik és integrálják az új technológiákat a különböző bűncselekmények elkövetésekor és új üzleti modellt alkalmaznak, amelyeknek az alapját egyre inkább az internet használata jelenti. A hagyományos szervezett bűnözői csoportok esetében is megfigyelhető a modern technológiák kihasználása, amely magában foglalja az interneten történő terjeszkedést mint például az illegális online kereskedelmet és a széles körben hozzáférhető, titkosított kommunikációs csator-

[52] Nagy Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. Belügyi Szemle 2012/6. 114-115. o.

[53] Conneller, Philip (2016): https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-Europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629 [2018.04.18.]

[54] Nagy Zoltán András: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1992/1. 26. o.

[55] Europol (2017): i.m. 35. o.

nák használatát és egyéb informatikai újításokat. Megállapítható, hogy az új technológiai vívmányok lényeges és maradandó hatással vannak a bűnözés természetére.

Az is kétségtelen tény, hogy az informatikai bűnözés egy hatalmas profit-orientált és szolgáltatás-alapú üzletté nőtte ki magát, azonban az még mindig nem világos, hogy ez a piac milyen mértékben van az egyes tradicionális szervezett bűnözői csoportok kezében, illetve mennyiben tekinthető az új típusú kiberbűnözői csoportok tevékenysége szervezett bűnözésnek egyáltalán. Ugyanis a szervezett bűnözés és az informatikai bűnözés kapcsolatára vonatkozóan még mindig nincs egy világos koncepció, különösen azért, mert nehéz a szervezett bűnözés hierarchikus, homogén struktúrájába az informatikai bűnözést beilleszteni. A „kiberbűnözői ipar" rendkívül erőssé és fejletté vált, azonban még mindig a fejlődésének korai szakaszában van, éppen ezért kevés a rendelkezésre álló adat, különösképpen a szervezettségi szintjére vonatkozóan.

Összességében elmondható, hogy az internet helyszínül szolgál mind a régi és mind az új típusú „szervezett" bűnözésnek, illetve mindkettő egymás mellett tud működni anélkül, hogy egymást zavarnák és ez köszönhető a virtuális tér speciális jellegének.

A jogalkotók, jogalkalmazók és a nyomozó hatóságok számára egyaránt kihívást jelent a titkosítást és anonimitást biztosító eszközök bűnelkövetési célú felhasználása, így különösen a kriptovatulák, az online feketepiacok és fórumok, melyek szabályozására szükség lenne, illetve a bűnüldöző szervek részéről kiemelten fontos, hogy biztosítsák az egymás közötti[56] és a magánszektorral való szoros együttműködést a hatékony fellépés érdekében.

Felhasznált Irodalom

Abadinsky, Howard: Organized crime. Ninth Edition, Wadsworth Cengage Learning, 2010.

Ambrus István: Egység és halmazat – régi dogmatikai kérdés új megközelítésben. Szeged, SZTE ÁJK, 2014.

Belegi József: A közbiztonság elleni bűncselekmények – Btk. XXX. fejezet. In: Kónya István (szerk.): Magyar büntetőjog I-III. – új Btk. – Kommentár a gyakorlat számára. 5. kiadás, HVG Orac Lapkiadó Kft. 2016.

[56] Lásd Simon Béla: A rendészeti szervek együttműködése a kiberbűnözés ellen. Nemzetbiztonsági Szemle 2018/1. 36-58. o.

Clough, Jonathan: Principles of Cybercrime. Cambridge University Press, 2015.
Csák Zsolt: Társas elkövetés, különös tekintettel a bűnszervezetre. In: Benisné Győrffy Ilona (szerk.): Negyvenegyedik Jogász Vándorgyűlés. Budapest, 2018.
Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2.
Europol: European Union Serious and Organised Crime Threat Assessment (SOCTA) – Crime in the age of technology. 2017.
Europol: Internet Organised Crime Threat Assessment (IOCTA) 2017.
Europol: The Internet Organised Crime Assessment (IOCTA) 2014.
Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8.
Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017.
Gyaraki Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények – A PIN kód megadása sikeres vagy biztonságos az internet?! Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012.
Kármán Gabriella – Mészáros Ádám – Tilki Katalin: Pénzmosás a gyakorlatban. Ügyészségi Szemle 2016/3.
Kim-wang, Raymond – Choo-Grabosky, Peter: Cybercrime. In: Paoli, Letizia: The Oxford Handbook of Organized Crime. Oxford University Press, 2014.
Korinek László: A szervezett bűnözés lényegi elemei. In: Harmadik Magyar Jogászgyűlés – Magyar Jogász Egylet. Budapest, 1996.
Korinek László: A technika fejlődése és a bűnözés. In: Borbíró Andrea – Inzelt Éva – Kerezsi Klára – Lévay Miklós – Podoletz Léna (szerk.): A büntető hatalom korlátainak megtartása: A büntetés mint végső eszköz – Tanulmányok Gönczöl Katalin tiszteletére. ELTE Eötvös Kiadó. Budapest, 2014.
Malas, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017.
McGuire, Michael: Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security. 2012.
Nagy Zoltán András: A 2013/40-es Uniós direktíva az informatikai rendszereket érő támadásokról.
Nagy Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula-Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIII. 2012.
Nagy Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. Belügyi Szemle 2012/6.
Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009.

NAGY Zoltán András: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1992/1.

SIMON Béla: A rendészeti szervek együttműködése a kiberbűnözés ellen. Nemzetbiztonsági Szemle 2018/1.

SZATHMÁRY Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/11.

TÓTH Mihály – KŐHALMI László: A szervezett bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára -Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016..

TÓTH Mihály: A bűnszervezeti elkövetés szabályozásának kanyargós útja. Magyar Jog 2015/1.

TÓTH Mihály: A gazdasági bűnözés és bűncselekmények néhány aktuális kérdése. MTA Law Working Papers 2015/4.

TÓTH Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009.

TÓTH Mihály: Gazdasági bűnözés és bűncselekmények. KJK-KERSZÖV Jogi és Üzleti Kiadó Kft. Budapest, 2002.

TROPINA, Tatiana: The evolving structure of online criminality. eucrim 2012/4.

NAGY ZOLTÁN ANDRÁS

A CSALÁS-JELLEGŰ CSELEKMÉNYEK AZ E-KERESKEDELEM KÖRÉBEN

1. Bevezetés

A katonai kutatás alapvetően a kommunikáció céljára hívta életre az internetet,[1] mely közel 30 évig az Egyesült Államok honvédelmi minisztériumának fennhatósága alatt működött a funkció bővülését követő különböző elnevezésekkel. Az 1980-as években a számítógépes hálózat megjelent Nyugat-Európában is, ez már a globalizálódás kezdete volt, igaz az európai és észak-amerikai hadseregeket kötötte össze. Az 1990-es évektől engedélyezték a hálózat kereskedelmi célú, egyszersmind civil hasznosítását.

1992-ben J.H. Snider and Terra Ziporyn szerzőpáros kiadta a „Future Shop: How New Technologies Will Change the Way We Shop and What We Buy" című könyvét. 1994-ben megjelent az első cég Pizza Hut. Közzétették az első banner hirdetéseket a hotwired.com honlapján. Az egyik a Zima nevű üdítőitalt, a másik az AT&T szolgáltatásait hirdette.1995-ben Amazon.com is megnyitotta virtuális áruházát, nem sokkal később az eBay is 1996-ban életre hívták az első netbankot NETBank nevén, amely 2007-ben zárta be „kapuját". Az első „fecskék" után ma már tömegesen találunk üzleti – kereskedelmi tevékenység folytatására szakosodott web-oldalt. A bevezetőben néhány fogalom tisztázása fontos.

Az elektronikus üzletvitel (electronic business, röviden: e-business) a számítógépes hálózatokon bonyolított gazdasági tevékenységek összessége. Tágabb fogalom, mint az elektronikus kereskedelem (electronic commerce, röviden e-commerce), mert magában foglalja a marketinget, a munkaügyi teendőket, a vevő tájékoztatást, a logisztikai és további feladatok végrehajtását. Az e-business területei a következők:

[1] Az internet (Internetworking System – hálózatok hálózata rövidítés). A szovjet szputnyik 1957-es sikeres fellövését követően kitört az USA-ban az ún. „szputnyik-sokk". Ezt ellensúlyozandó, többirányú fejlesztésbe kezdtek. Ezek egyike volt az, hogy a hadserege vezetésének megbénítását megakadályozandó, több vezetési pontot alakítottak ki. Ezeket földalatti kábellel kötöttek össze. Majd egyre több katonai és civil kutatóintézet és egyetem csatlakozott a hálózatra, míg végül szétvált a katonai és civil hálózatra, amely utóbbit 1993-tól lehet szabadon használni.

Business to business (röviden: B2B): az eladó is vállalat, vállalkozás (szervezet), és a vevő is vállalat, vállalkozás (szervezet). Két vagy több cég, intézmény között létrejövő elektronikus marketing, logisztikai, értékesítési és egyéb relációk. Legjellemzőbb területei a nagykereskedő és kiskereskedő között kereskedelmi kapcsolat, illetve a vállalkozások egymás között kötött üzleti célú megállapodásai, azok teljesítése, marketing folytatása stb.

Business to consumer (B2C): a vállalat, vállalkozás a fogyasztó felé fordul áru-, szolgáltatás nyújtása, marketing (reklám, kérdőív, nyereményjáték formájában is), kommunikáció és egyéb üzleti célból.

Cwonsumer to business (C2B): a fogyasztó keresi a vállalkozásokat, vállalatokat, áruvásárlás, szolgáltatás rendelése, igénybe vétele (web-shopok, utazási irodák, autóbérlés stb.) céljából.

Consumer to consumer (C2C): a fogyasztó a fogyasztóval áll üzleti, kereskedelmi kapcsolatban, például second hand oldalakon, vásárok hirdetésével, egyéni eladásokkal.

Léteznek aztán további relációk:

Az e-businessbe a kormányzat, önkormányzat, államigazgatás is beléphet, pl. koncessziós pályázatok, közbeszerzések kiírása, állami megrendelések stb. (A2B), koncessziós-, közbeszerzési pályázatok benyújtása, állami megrendelések teljesítése stb. (B2A), adó-, vám-, illeték kiszabása, beszedése (A2C, A2B), fizetése, hivatalos okiratok intézése, ellenértékük megfizetése céljából (B2A, C2B).

Továbbá – sajnos, realitás – a Criminals to Criminals (C2C) viszonylat is, a külön kliens programmal elérhető Darkneten virtuális valutáért fegyverek, hamis okiratok, pornográf-, pedofil fotók, videók, az e-mail-címek, személyes adatok, kábítószer és más tárgyak, eszközök adásvétele, a botnetek, a bérgyilkosság bérlése, bűnözők, terroristák titkolt kommunikációja és más ügyletek.

Az elektronikus üzletvitelnek része az elektronikus kereskedelem, amely a távollévők között, elektronikus eszközök által tett olyan jogilag releváns cselekményeket foglalja magában, amelyek egyedileg meghatározható jogalanyok között polgári jogi jellegű jogviszonyt hoznak létre, feltéve, hogy a jogszabály az elektronikus kereskedelemre vonatkozó rendelkezések alkalmazását nem zárja ki.[2] E teljeskörű, absztrakt definícióból kiszűrhető, hogy az e-kereskedelem a polgárjogi szabályok szerinti zajló eladó és vevő közötti adásvételre, szolgáltatás nyújtására koncentrál.

Az e-kereskedelem nem korlátozódik a számítógépes hálózatokon (interneten, extraneten, intraneten) folyó kereskedelmi tevékenységekre, idetartoznak a külön-

[2] KONDRICSZ Péter – TÍMÁR András: Az elektronikus kereskedelem jogi kérdései. Budapest, KJK-Kerszöv. Jogi és Üzleti Kiadó, 2000. 71. o.

böző automaták (a jegykiadó automatáktól az édességet, üdítőket áruló automatákig), a mobiltelefonon közvetlenül vagy valamely applikáción keresztül történő áru-, szolgáltatásrendelés és fizetés.

Jelen fejezetünk az interneten zajló kereskedésre fókuszál.

2. Az e-kereskedelemmel összefüggő csalás-jellegű tevékenységek típusai

2.1. A megtévesztő tartalomközlésekkel megvalósuló csalás-jellegű tevékenységek[3]

Az internet weboldalain, az elektronikus hirdetőtáblákon (bulletin boards), hírcsoportban (news-groups), a különböző közösségi oldalakon, a Twitteren, Messengeren, chat-oldalakon, saját weboldalon, más weboldalak fórum rovataiban, az FTP-, a goopher-, a telnet-hálózatokon, az intra-, és az extraneten tehetők közzé árut, szolgáltatást hirdető tartalmak, szövegben, képben, valamint ezekhez csatolt audió-, vagy videofájlban. Továbbá küldhetők közlések, hirdetések[4] egy meghatározott személynek, illetve korlátlan számú személynek elektronikus levélben (e-mailben). E számos közlésre alkalmas oldalon egyaránt olvashatók – csak az üzleti – kereskedelmi tartalmakat tekintve – valódi és megtévesztő információk.

2.1.1. A csaláshoz (Btk. 373.§) legközelebb álló tartalomközléssel elkövethető bűncselekmény a Btk. 412. §-ba ütköző és e szakasz szerint minősülő „piramisjáték szervezése" bűncselekmény. A „szervezés", mint elkövetési magatartás felölheti a számítógépes hálózaton történő jellemzőn írásbeli tájékoztatást (pl. a szabályok ismertetését, a kis befektetéssel nagy nyereséget hozó megtévesztő ígéretet stb.), ami – implicite – felhívást, mint verbális előkészületi magatartás, vagy ha sikeres a felhívás, akkor az rábírás, mint felbujtói magatartás.

Nem csupán a piramisjáték kezdeményezője tekintendő szervezőnek, hanem azok is, akik újabb személyeket szerveznek be a játékba, azaz, akik megosztják a piramisjátékra vonatkozó tartalmakat, kivéve azon felhasználókat, akik a játéktól való tartózkodásra hívják a figyelmet, akik leleplezik a játék valódi természetét.

[3] Nagy Zoltán: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1. 1992/1. 22-26. o.

[4] Nagy Richárd: A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései. Belügyi Szemle 2018/7-8. 87. o.

2.1.2. Megtévesztő tartalomközlés vonatkozhat továbbá egyfelől rossz minőségű termékre is.[5] A rossz minőség fogalmát a Büntető törvénykönyv egy speciális – csak e szakaszra releváns – értelmező rendelkezésben határozza meg, melynek értelmében: rossz minőségű a termék, „ha a jogszabályban vagy az Európai Unió közvetlenül alkalmazandó jogi aktusában előírt biztonságossági vagy minőségi követelményeknek nem felel meg, ilyen előírás hiányában akkor, ha a termék rendeltetésszerűen nem használható, vagy használhatósága jelentős mértékben csökkent." (Btk. 415.§ (6) bekezdése).

Ha a forgalomba hozatal megtörténik, akkor a tevékenység a Btk. 415.§ (1) bekezdésébe ütköző és egyéb minősítő körülmények hiányában ugyanezen bekezdés szerint minősülő rossz minőségű termék forgalomba hozatal bűncselekménye valósul meg.[6]

Ugyanakkor a termék számítógépes hálózaton történő felkínálása megvételre a bűncselekmény előkészületi cselekményének (Btk. 415.§ (3) bekezdés) minősül.

A jogalkotó a fogyasztói érdekek védelme, a termékek minőségbiztosításának fontossága miatt a gondatlan bűnelkövetést is szankcionálja (Btk. 415.§ (4) bekezdés).

Ugyanakkor a forgalmazás felhívója büntetlenségét biztosítja a törvényhozó, ha mihelyt tudomást szerez a termék rossz minőségéről, mindent megtesz azért, hogy a rossz minőségű termék a birtokába visszakerüljön (Btk. 415.§ (5) bekezdése).

Mivel megtévesztő tartalomközléssel valósul meg a rossz minőségű termék forgalomba hozatala, így – értelemszerűen – a csalás (Btk. 373.§) bűncselekményéhez való viszonyát tisztáznunk kell. A rossz minőségű termék forgalomba hozatala bűncselekmény tárgyi oldalán eredményt, in concreto kárt nem határoz meg a törvényhozó a tényállásban, míg a csalás bűncselekménye tárgyi oldalán a kár tényállási elem. Ha azonban a jogsértő cselekmény elkövetésével kár is keletkezik, és a csalás büntetési tétele az adott esetben magasabb, a konszumpció elve alapján kizárólag csalás megállapítására kerülhet sor.[7]

Még egy megjegyzés, amennyiben a rossz minőségű termék egyben olyan termék, amely az adott közfogyasztási cikk vonatkozásában valamilyen rendellenességet mutat (pl. megromlott, a gyártási technológia miatt vagy tárolása során vált rendellenessé), és ezzel egészségre is káros, akkor ártalmas közfogyasztási cikkel visszaélés bűncselekményt (Btk. 189. §) kell felhívni. Megjegyzendő, hogy ennek

[5] Tóth Mihály: Gazdasági bűnözés és bűncselekmények. Budapest, KJK-Kerszöv., 2002. 193-200. o.

[6] Lásd ehhez Szathmáry Zoltán: A hamis termékek forgalmazásával elkövetett iparjogvédelmi jogok bizonyításának nehézségei. Ügyészek Lapja 2015/2. 5-15. o.

[7] Tóth Mihály: Rossz minőségű termék forgalomba hozatala. In: Tóth Mihály – Nagy Zoltán (szerk.): Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2014. 569-571. o.

a bűncselekménynek nincs előkészülete, így e bűncselekmény csak a forgalomba hozatallal jön létre (Btk. 189.§ (2) bekezdése).

2.1.3. Másfelől az áru valamely „lényeges tulajdonságai" tekintetében is lehet megtévesztő a tartalomközlés.[8]

Ez esetben a Btk. 417.§ (2) bekezdése szerint minősülő és ugyanezen szakasz szerint büntetendő fogyasztók megtévesztése bűncselekmény jön szóba. E bekezdésben a bűncselekmény elkövetési magatartása, jelesül a „megtévesztésre alkalmas tájékoztatás" számítógépes környezetben is releváns lehet. A lényeges tulajdonság absztrakt fogalmát egy speciális értelmező rendelkezés részletezi:

– az áru összetétele, műszaki jellemzői és az árunak az adott célra való alkalmassága,
– az áru eredete, származási helye,
– az áru tesztelése, ellenőrzöttsége vagy annak eredménye (Btk. 417. (4) bekezdése).

A bűncselekmény súlyosabban minősül, és akár három évig terjedő szabadságvesztéssel is büntetendő, ha az áru egészségre vagy környezetre gyakorolt hatásával, veszélyességével, kockázataival vagy biztonságosságával kapcsolatos jellemzőivel összefüggésben követik el.

A fogyasztók megtévesztése bűncselekmény tényállásban esetleges tárgyi elemként szerepel a hely, in concreto a „nagy nyilvánosság". A magyar büntetőjogban az 1999. CXX. törvény a nagy nyilvánosság fogalmát kiterjesztette az elektronikus hírközlési hálózatokra is, így a számítógépes hálózatok is ideértendők. A nagy nyilvánosság jelen fogalma a Btk. értelmező rendelkezésének 22. pontjában olvasható, – természetesen – az elektronikus hírközlő hálózat fogalmával együtt. Így a fogyasztók megtévesztése bűncselekménye ide idézett alapesete (2) bekezdése is csak akkor valósul meg, ha azt nagy nyilvánosság előtt, pl. számítógépes hálózatokon keresztül követik el.

2.1.4. Az áru eredetére vonatkozó hamis vagy csupán részben valódi tartalomközlés is megvalósíthat bűncselekményt, ha a vámellenőrzés alól elvont nem közösségi árut, jövedéki adózás alól elvont terméket, vagy lopásból, sikkasztásból, csalásból, hűtlen kezelésből, rablásból, kifosztásból, zsarolásból, jogtalan elsajátításból vagy orgazdaságból származó dolgot kínálnak eladásra. Amennyiben az eladó a dolog az elkövető birtokában van, és ezért tudja az árut értékesíteni, akkor orgazdaságért

[8] Tóth (2002): i.m. 219-228. o. Tóth Mihály: Fogyasztók megtévesztése. In: Tóth Mihály – Nagy Zoltán (szerk.): Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2014. 572-575. o.

(Btk. 379.§) felel, amennyiben nincs a bűncselekményből származó dolog a birtokában, de tud arról, hogy lelhető fel vagy rendelésre elérhetővé válik, akkor bűnpártolásért (Btk. 282.§) felel az elkövető.

Az orgazdaság elkövetési tárgyai egyfelől a közösségi áruk, melyek:

– olyan áruk, amelyeket teljes egészében a Közösség vámterületén állítottak elő/jöttek létre (és nem tartalmaznak harmadik országból importált árukat),
– olyan harmadik országból importált áruk, amelyeket szabad forgalomba bocsátottak,
– olyan áruk, amelyet vagy harmadik országból importált és szabad forgalomba bocsátott árukból, vagy a Közösség területén létrejött/előállított árukból és harmadik országból importált és szabad forgalomba bocsátott árukból állítottak elő/jöttek létre.

A nem közösségi áruk tehát, olyan áruk, amelyek eltérnek a közösségi áruktól.

Másfelől a jövedéki termékek, mint elkövetési tárgyak:

– az ásványolaj,
– az alkoholtermék,
– a sör,
– a bor,
– a pezsgő,
– a köztes alkoholtermék,
– a dohánygyártmány.[9]

A teljesség igényével: ha a jövedéki termék az elkövető birtokában van, és értékesíti az árut, akkor költségvetési csalást (Btk. 396.§) követi el, azonban, ha az elkövető nincs a jövedéki termék birtokában, de tud arról, hogy az hol lelhető fel vagy rendelésére elérhetővé válik, akkor bűnpártolásért (Btk. 282.§) felel.

2.1.5. Megtévesztő tartalomközlés lehet olyan termékre vonatkozóan, amely a termék valódi mivoltát, tulajdonságait részben vagy egészben leplezi. E körbe tartozhatnak a jogszabályokban tiltott termékek.

A termék kábítószernek minősülő elegy, szer, tabletta stb. összetételének elhallgatásával megtéveszti az érdeklődő felhasználót, akkor a kábítószert áruló személy, ha a kábítószert forgalomba hozta, akkor a Btk. 176.§ (1) bekezdésébe ütköző és egyéb minősítő körülmények hiányában e bekezdés szerint büntetendő kábítószer-

[9] 2003. évi CXXVII. törvény a jövedéki adóról és a jövedéki termékek forgalmazásának különös szabályairól 3.§ (2) bekezdés

kereskedelem bűntettét követi el. Amennyiben a forgalomba hozatal nem valósult meg, akkor pedig a bűncselekmény előkészülete (Btk. 176.§ (6) bekezdés) valósul meg. Továbbá a kábítószer forgalomba hozatalához szükséges számítógépes háttér biztosítója delictum sui generis bűnsegédként felel (Btk. 176.§ (4).

Hasonló a szabályozás az új pszichoaktív anyag forgalmazása esetén (Btk. 184.§ (1) bekezdés). Tehát büntetendő a dizájner drogok forgalmazásának előkészülete (Btk. 184.§ (6) bekezdése), és a forgalmazáshoz nyújtott delictum sui generis bűnsegély is (Btk. 184.§ (4) bekezdése).

A doppingszerek[10] esetében a Büntető Törvénykönyv a forgalmazói magatartásokat rendeli büntetni (Btk. 185.§ (2) bekezdése). Szankcionált a forgalmazás előkészülete is (Btk. 185.§ (4) bekezdés).

A fenti tilalmakhoz hasonló a hamis, hamisított vagy Magyarországon nem engedélyezett egészségügyi termékek forgalmazása büntetni rendeltsége (Btk. 186.§ (1) bekezdés). Úgyszintén tiltott a forgalmazás előkészülete is (Btk. 186.§ (4a) bekezdés).

Ezekben az esetekben bár lehet megtévesztő a tartalomközlés a termék tulajdonságára, összetételére, más jellemzőjére vonatkozóan, sőt a potenciális fogyasztók tévedésbe ejtésének vagyoni haszonszerzési célja is lehet, de ez nem csalásként (Btk. 373.§) értékelendők, hanem a fentebb említett tényállások hívandók fel.

2.1.6. Ismert olyan megtévesztő és haszonszerzési célú tartalomközlés, amely nem bűncselekmény, mivel előkészülete nincs, kísérleti szakaszba lépése pedig látens marad, és csak a befejezett bűncselekmény észlelhető.

Az internetes pénzügyi visszaélések közül a leghíresebb-leghírhedtebb az ún. nigériai levelek („Advance Fee Fraud", vagy „419 Fraud" [Four-One-Nine], – a 419-es szám a nigériai büntető törvénykönyv idevonatkozó rendelkezésének a száma) néven elhíresült csalássorozat.

Lényege az, hogy a gyanútlan felhasználó saját e-mail címére kap egy levelet, amelyben egy magas rangú nigériai hivatalnok, kormánytag stb. leszármazója a gyanútlan felhasználónak (egy szívhez szóló levélben) arról panaszkodik, hogy apja halála után a családi vagyont zárolták, és annyi pénze sincs, hogy az ügyvédi, és egyéb díjakat, – amelynek fejében a vagyont vissza tudná szerezni – kifizesse. Így pénzt kér egy nigériai bankszámlára. Természetesen a visszaszerzett vagyonból busásan „kárpótolná" a neki segítőt.[11]

Ezekhez hasonló a nemrégiben feltűnt és talán most is „játszott" holland lottó. Ebben az esetben a gyanútlan felhasználó szintén a saját e-mail címére kap egy levelet,

[10] Lásd bővebben: Nagy Zoltán András: Sport és büntetőjog. Pécs, Kódex Nyomda, 2014.
[11] http://www.webmutato.hu/webmix/uzlet/vigyazat.htm [2018.03.31.]

amelyben közlik vele, hogy nyert Hollandiában a lottójátékon, ám a nyeremény átvétele előtt ki kellene fizetni a nyereményadót, meg valamilyen járulékos költséget. Tehát a megtévesztés abban áll, hogy nyereményt ígérnek bizonyos pénzösszeg megelőlegezését követően.[12] Már spanyol, sőt svájci lottóként is ismert ugyanez a szisztéma.

Újabb hasonló próbálkozás volt, amikor a „nigériai levelek" példáját követve a Dél-Afrikai Köztársaságból érkeztek megkeresések magyar felhasználókhoz.[13]

Mivel a csalás bűncselekményének (Btk. 375.§) az előkészülete kívül esik a büntetni rendeltségen, így ezek a megtévesztő tartalomközlések legfeljebb erkölcsileg helyteleníthetők, hiszen csupán a megtévesztésből nem keletkezhet kár.[14]

2.2. A tranzakció során megvalósuló megtévesztések

Az e-kereskedelem folytatásához – általában – e-boltok „nyitása" szükséges feltétel. Az ügylet távollévők között köttetnek.[15] A tranzakcióra a távollévők között kötött szerződés külön szabályai irányadók. Ennek egyik legfontosabb szabálya fogyasztó elállásának a lehetősége. A felhasználó egyoldalúan visszaléphet és a termék visszaküldése esetén követelheti a kereskedőtől az általa kifizetett összeg visszatérítését.[16] Az elállási jog kompenzálja azt, hogy a vásárlás előtt nem volt lehetőségünk a termék megvizsgálására, kipróbálására, illetve üzembe helyezésére.

Az e-boltokban történő vásárlás előtt a felhasználónak regisztrálnia kell egy azonosítóval és egy jelszóval, majd ezen adatokkal tud belépni az e-boltba. Ott a kiválasztott árut egy virtuális kosárba helyezi, majd kiválasztja a szállítási címet (a felhasználó lakcímére, a pick-pontra vagy az értékesítőhelyre), majd a fizetés módját (utánvéttel a teljesítés helyén, bankkártyával on-line, átutalással, az eladó valós térbeli telephelyén, raktárában, készpénzzel vagy kártyával stb.), majd a vevő a regisztráció során megadott e-mail címre, telefonra stb. kap egy visszaigazolást a vásárlásról.

Az e-boltok virtuális áruházak[17], amelyeknek több előnyét már megtapasztalhattuk és fejlődésüknek is emiatt töretlen:

---

[12] http://index.hu/tech/jog/holland0902/ [2018.03.31.]

[13] Lásd Clough, Jonathan: Principles of cybercrime. Second Edition. Cambridge University Press, 2015. 209-212. o.

[14] Erdősy Emil – Földvári József – Tóth Mihály: Magyar Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2004. 507. o.

[15] 45/2014. (II. 26.) Korm. rendelet III. fejezete

[16] 45/2014. (II. 26.) Korm. rendelet III. 24. §

[17] Érdekességként megemlítendő, hogy a webáruházakra nézve veszélyt jelenthetnek az ún. DDoS-támadások, melyek jelentős bevételkiesést és presztízs veszteséget eredményezhetnek a támadással érintett cégnél. Lásd Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1. 70. o.

– A valós térbeli üzleti lehetőségekkel szemben a teljes választék prezentálható.
– Nélkülözhető egy üzlet-, irodahálózatot fenntartása, elegendő egy raktáráruház, központi irodára, esetleg elég egy logisztikailag jól szervezett hálózat részének lenni, ahol közvetítő tevékenység is folytatható, kevesebb élőmunka szükséges a tevékenységhez.
– Költséghatékony, ami olcsóbb árakat is jelenthet, pontosabban jelenthetne, ha a szállítási költségek nem drágítanák meg az értékesítést.
– Mivel nincsenek üzletei a vállalkozásnak, nem kell azokat folyamatosan feltölteni, így az állandó szállítások hiányában ez az értékesítési forma egyben környezetbarát is.
– Gyakorlatilag non-stop „nyitva tartással" működnek az e-boltok.
– Mivel a Föld minden tájékán működnek e-boltok, így a vevő előtt megnyílik az egész világ.
– Gyors üzletkötés lehetősége adott („one click order").
– A vállalkozás számára a reklám lehetőség saját web-oldalán korlátlan, ezt segíthetik linkek, nyereményjátékok stb.
– A vállalkozás a piackutatáshoz, marketing tevékenységének eredményesebbé, sikeresebbé teheti saját felhasználású kérdőíve elérhetőségével web-oldalán.
– A vevőnél a kényelmi szempontok elvitathatatlanok, karos székből választhat és házhoz szállítják az általa rendelt árukat.
– Tegyük hozzá nem kevés malíciával, hogy az is előnye az e-boltoknak, – mivel fizikailag nincsenek jelen a vevők, – így nem lopnak, nem lophatnak a boltból, ami ugyebár a valós térbeli boltoknál, üzleteknél reális veszély.

Az e-boltok térhódításukkal ma még kiegészítik a valós térben található kereskedelmi egységeket, és biztosak lehetünk abban, hogy nem is szoríthatja ki azokat, hiszen vannak olyan hátrányai az e-boltoknak, amelyeket nem lehet kiküszöbölni.

– A vevő nem kerül fizikai kapcsolatba az általa kinézet vagy választott termékkel, így (cipők, ruhadarabok nem próbálhatók fel, használt gépjármű vétele kifejezetten „zsákbamacska").
– Hátrány az is, hogy az értékesítés során a vevő és az eladó közötti kontextus személytelen, elmarad az eladó segítőkészsége, rábeszélése"
– Nem minden áruféleség értékesíthető, illetve értékesíthető a vevő számára biztonsággal (pl. a törékeny áruk), továbbá frissensült élelmiszerek (pl. pizza, egyéb péksütemény), ha a vevő frissen is kívánja elfogyasztani, aki az eladónak és megrendelőnek időben – viszonylag – közel kell lenniük egymáshoz.

A veszélyek az e-kereskedelem hátrányaiban rejlenek. Az eladó oldalán jelentkező gond az, hogy nem kerül fizikai kapcsolatba a vevővel és a vevő bankkártyájával. Egyfelől nem lehet biztos abban, hogy a megrendelő valós személy-e vagy valós e-mail-címmel regisztrált-e. Másfelől az eladó a vevő által használt bankkártyával sem érintkezik, és szintén nem lehet biztos abban, hogy a bankkártya, mivel fizettek, valódi-e és, ha valódi is a tényleges kártyabirtokosé vagy sem.

A vevő is aggódhat azért, hogy megkapja-e az árut, illetőleg az áru az-e, amit rendelt, az áru nem bűncselekményből származik-e, nem szenved-e más jogi vagy minőségi fogyatékosságban.

Az üzletkötés gyorsasága és egyszerűsége iránt igényt kell a biztonság követelményével összeegyeztetni.

2.2.1. Card-present csalás[18]

Hazánk pénzügyi történetéből – gazdasági fejletlensége miatt – a „csekk-korszak" kimarad és a fejlett piacgazdaságok technikai evolúciójában a bankkártyák korszakába csöppent. Először 1988-ban jelent meg az első, még devizaszámlához kapcsolt, egy évvel később a csekkhez kötött kártya. Ugyanebben az évben került forgalomba az első ún. ATM – kártya is.

Ma Magyarországon hét és félmillió körüli különféle banki műveletek végrehajtására szolgáló bankkártya,[19] valamint több százezer nem a bankok által kibocsátott plasztiklapok kerülnek forgalomba, így az American Express (Amex)-kártyái, valamint olajtársaságok üzemanyagkártyái, kereskedelmi egységek kártyái stb.

A bankkártyák funkciói folyó-számlakezelés, készpénzfelvétel automatából vagy a pénztárból, készpénz nélküli vásárlás, átutalás, vásárlás az interneten keresztül, hitelfelvétel, csekkgarancia stb. Sőt, – saját tapasztalatból merítve – az Egyesült Királyságban a kártyával történő vásárlás helyén pénzfelvételre is van mód (ez az ún. cash – back funkció), azonban e szolgáltatás hazánkban még ismeretlen.

A legkülönfélébb kereskedelmi, vendéglátó, idegenforgalmi helyek, amelyek vállalják a bankok által kibocsátott kártyák elfogadását ezzel az ügyfél számára lehetővé teszik a készpénz nélküli vásárlást vagy szolgáltatás igénybe vételét. A plasztiklap mára munkahelyi-, uszoda-, könyvtár-, golf- és jachtklub, stb. belépő, többféle

[18] Lásd részletesen: Mezei Kitti – Tóth Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós – Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017. 297-308. o.; valamint Ambrus István – Deák Zoltán: Súlyponti kérdések a bankkártyával kapcsolatos bűncselekmények köréből. Belügyi Szemle 2011/2. 85-103. o.

[19] http://www.klikkbank.hu/lakossagi/20051026mar75.html [2017.09.30.]

törzsvásárlói (sőt multi-) kártya. Nem kicsiny feladatot ró ránk az egyre növekvő számú különböző azonosítók (PIN-kódok, jelszavak stb.) megjegyzése vagy legalábbis annak azonnali ismerete, hogy hová írtuk fel.

A készpénzkímélő kártyák elvitathatatlan előnyei, amelyek tények (pl. kényelmes, prompt nagyobb vásárlások lehetősége stb.) mellett inkább a pénzintézetek és a munkáltatók járnak jól a fizetések bankszámlára történő utalással. Tényszerűen, a pénzintézetek azért, mert a kártyaszámlára történő munkabér átutalással, pótlólagos forráshoz jutnak havonta, hiszen a számlára utalt pénzt nem egyszerre, hanem többszöri alkalommal veszik le az ügyfelek, továbbá azzal, hogy a kártyabirtokosok sokszor nem merítik ki számlájuk egyenlegét (marad néhány száz-, néhány ezer forint a több millió kártyabirtokos számláján). Ezentúl valamennyi bankműveletért, így általában a 2-nél többszöri pénzlevételért, számlavezetésért, átutalásért, átvezetésért pénzkezelési és egyéb költségeket számolnak fel, amelyek tisztes nagyságrendet is elérhetnek. De jól járnak a munkáltatók, mert megmenekülnek a pénzkivétellel, pénzőrzéssel, és a kézi kifizetéssel összefüggő költségektől.

Az ügyfelek járnak a legrosszabbul, mivel a bankkártya őrzése, továbbá a bankkártyák használatához „sok kicsi, sokba kerül" költségek őket terhelik. Nagy valószínűséggel a közszférában senki nem kapja kézhez a jogszabályban, vagy munkaszerződésben meghatározott bruttó bérből következő nettó bért, csak a banki költségekkel csökkentett nettó bért. Bár a munkáltatók a bankkártya költségek ellensúlyozására törekednek egy minimális összeggel, amely az ügyfelek banki veszteségeinek csupán kis részét fedezik.

Reális probléma az is, hogy a bankkártya elvesztése, ellopása jóval nagyobb kárt okozhat[20] az ügyfél számára, mintha a pénztárcáját elhagyta vagy ellopták volna őrizetéből. A bankkártyán ugyanis az egész havi bevételünk szerepel, míg pénztárcánkban általában az aktuális áruvásárlás, vagy szolgáltatás igénybevételének becsült költsége van némi rátartással, és nem az egész havi fizetésünk egyszerre. Napjainkban jellemzően a „kisemberek" viselik mások gazdagodásának, multik és a politika erőteljes, önös érdekérvényesítésének, a rossz gazdasági, politikai döntéseknek káros következményeit, és tőlük várják, hogy feláldozzák életüket a gazdasági, politikai érdekekért, terület- vagy energiaforrás szerzéséért.

A bankkártyák számának és a velük végzett műveletek elterjedésével egy időben a kártyákkal történő visszaélések lehetőségei folyamatosan bővülnek. A bankkártyák biztonsági rendszere mindig is a bűnözők sikeres módszerei mögött marad, ami általában természetes folyamat.

[20] Például külön érdekesség, hogy sor került a rendőrségi állomány ismereteinek a vizsgálatára a készpénz-helyettesítő fizetési eszközök használatával kapcsolatban. Lásd bővebben: SIMON Béla: A rendőrségi állomány felkészültsége a kiberbűnözésre. Hadtudományi Szemle 2018/1. 394-396. o.

A kártyakibocsátók ennek megakadályozására több- és eltérő fokozatú biztonsági megoldásokat dolgoztak ki, és alkalmaznak:

- A kártyakibocsátó által használt nemzetközi logo (EC/MC, Visa).
- A kártyán levő dombornyomás és annak valódisága. Több elektronikus kártyán nincs dombornyomás (pl. Cirrus, VISA Electron, internetes vásárlásra kibocsátott).
- Bonyolult kártyaszám alkalmazása: meghatározott számkombinációk (bank, ügyfél, kártyatípus stb.) találhatók a kártyákon. A Mastercard kártyaszáma 16 számból áll, és 51, 52, 53, 54, vagy 55-tel kezdődik. A Visa kártyaszámok 13 vagy 16 számjegyből állnak, és 4-sel kezdődnek. Az American Express kártyaszáma 15 számból áll és 34 vagy 37 a kezdete. A Diners Club kártyaszáma 14 számból áll, és 30, 36, vagy 38 a kezdete. A VISA kártyaszám első négy számjegyét a szám alatt vagy felett nyomtatva is megismétlik, míg a Mastercardon, a hátlapon, az aláírási panelben is jelzi a kártyaszámot.
- Egyedi PIN-kód generálása vagy választása. E PIN-kódok különböző jogellenes (megtévesztés mint például a social engineering technikák alkalmazása), erőszakos cselekményekkel (kényszer, fenyegetés, zsarolás stb.) kikényszeríthetők a kártyabirtokostól.[21]
- Hologramos jelek alkalmazása.
- Csak UV-lámpával látható jelzések.
- A megjelölt lejárati dátum megakadályozza, hogy a kártyát érvényességi idején túl is használják.
- A kártya hátoldalán szereplő aláírás.
- Először a videókazetták mágnesszalagja méretével teljesen megegyező mágnesszalag alkalmazása adatrögzítésre, amely gyerekjátékká tette a bankkártya klónozását, a mágnesszalagon szereplő adatok „ellopását". Ezt a nagyon amatőr technikai megoldást váltotta fel a chip, majd nagyon rövid időn belül a biometrikus azonosítás bevezetése.
- Online kapcsolat kiépítése a kártyakibocsátók- és az elfogadóhelyek között, ezzel online tranzakciók lebonyolítása, amellyel legalább az offline csalás lehetőségeit szűrhetik ki.
- Azonnali SMS-értesítés a bankkártyával történő fizetésről.
- A kártyahasználat identifikálása, amellyel a szokatlan tranzakciók kiszűrhetők.
- A gyanús ügyfelek nyilvántartása, kizárása a kártyatársaságoknál, bankoknál.

[21] Gyaraki Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012. 243. o.

A kereskedelmi és a vendéglátóhelyeken történt vásárláskor a kártyabirtokos aláírásával hitelesíti a kártyával történő vásárlást. Vajon ellenőrzik-e minden esetben a kereskedők az aláírást, és ki tudják-e szűrni a hamis aláírásokat? Sajnálatosan, nem minden esetben győződnek meg arról, hogy a kártyán, illetőleg a vásárlást igazoló blokkon hasonlít-e az aláírás. Általában a lehúzást követően gyorsan visszaadják a vásárlónak, és sok esetben a tranzakció vége előtt már a következő vásárló áruit olvassák be a pénztárgépbe.

A kis értékű, Magyarországon az 5 000 forintos vásárlási limitig nem szükséges PIN-kód begépelése a terminálba, ami kényelmi szolgáltatás, ám visszaélés esetén a biztonság ezzel nullára csökkent.

Jelen tanulmányunk csak a bankkártyával fizetéssel összefüggő visszaélésekre koncentrál,[22] így kimaradnak az ATM-elleni támadások különböző fajtái és lehetőségei (közvetlen pénzszerzés, a bankkártya fizikai megszerzése illetőleg a bankkártyán található elektronikus adatok megismerése stb.).

Kártyaelfogadással kapcsolatos potenciális visszaélések:

- Kártyaelfogadás fiktív (ál-) üzletben. Az elkövetők hamis, hamisított okiratokkal olyan kereskedelmi üzletet nyitnak, amelyek bankokkal szerződést kötnek kártyaelfogadásra. Néhány heti vagy havi forgalom után, bevárva a banktól átutalt összegeket az álkereskedők megszüntetik vállalkozásukat.
- Az engedélyeztetéshez szükséges szigorú szabályok szűrhetik ki a csalókat.
- „Csalárd összejátszás" a jogosulatlan vásárlókkal: a kereskedő tudva arról, hogy hamis, hamisított vagy lopott kártyát használnak fel, elfogadja azt és igazolja a vásárlást. Nyilván a kereskedő „tévedésére", „tökéletesnek látszó hamis bankkártyára" hivatkozva hárítaná el a felelősségét.
- A kártyalehúzások megtöbbszörözése. Ebben az esetben „fizetéskor" a vásárolt összeg többszörösével terheli meg a vevő kártyaszámláját. A kártyabirtokos, ha kiadta a kezéből a bankkártyáját pl. elegáns étteremben, benzinkútnál akkor szembesülhet azzal, hogy kártyáját többször lehúzták, illetve a kártya hátoldalán levő titkos kódot lemásolták.
- A fizetésről szóló azonnali SMS-értesítés rögtön jelzi, ha a kártyát többször lehúzták.
- A kártya adatainak lemásolása ellen csak úgy védekezhetünk, ha a kártyát ki sem adjuk kezünkből, még fizetéskor sem.

[22] Goodman, Marc: Future Crimes. London, Transworld Publishers, Corgi Book, 2016. 302-303. o. Senker, Cath: Cybercrime and the Darknet. London, Arcturus Holdings Ltd., 2017. 42-43. o. Nagy Zoltán András: Bűncselekmények, számítógépes környezetben. Budapest, Ad-Librum, 2009. 153-173. o.

– A kártyalehúzás többszörözése abból a célból, hogy a kártyán szereplő adatokat megismerjék („klónozás", „korábban stemplizés").

A kártya-felhasználás során megvalósítható visszaélések:
– A kártyabirtokos visszaélései között korábban volt gyakori a fedezettúllépés: a kártyabirtokos szándékosan többet költ, mint amennyi a kártyaszámláján van. Csak offline terminálon keresztül történő vásárlásnál valósítható meg.
– Más személy kártyájával megvalósítható visszaélések:
– Elvesztett vagy ellopott bankkártyákkal a PIN-kód hiányában kis értékű vásárlásokkal az eredeti kártyabirtokosnak kárt okozó visszaélés, sőt a PIN-kód ismeretében még nagyobb anyagi kár okozható, a bankkártya letiltásáig.
– Hamis vagy hamisított kártyák használata esetén egy már létező kártyáról készített az «klónozott" kártyával történik a fizetés, ebben társ lehet a kereskedő is. Vagy még azelőtt, mielőtt a bankkártya birtokos átvette volna a kereskedelmi banktól a kártyáját klónozták a banki munkatárssal összejátszó elkövetők. A bankkártya szigorú zárt borítékban történő csomagolása ez utóbbit kiszűri.

2.2.2. A card-not-present csalás

E csalási formáról akkor beszélünk, amikor a tranzakciónál nincs jelen a kártya.[23] Az online, a telefonon, mobiltelefon applikációján keresztül történő áru- vagy szolgáltatás rendelés kifizetésénél nincs jelen a bankkártya.

A veszélye – tehát abban van –, hogy az eladó nem vizsgálhatja a bankkártya tulajdonosát, a bankkártya valósnak tűnik, hiszen fizetéskor a bankkártya validitását ellenőrzi a befogadó bank rendszere. Bár a bankkártya lehet klónozott is.

A bankkártya ma már multifaktoros védelme (elektronikus és biometrikus azonosítók, a tranzakciók és az identitás összekapcsolása, figyelemmel kísérése és más megoldások) sem nyújtanak teljeskörű biztonságát a card-not-present csalások ellen.

A bankkártya érvényességét a kártyabirtokos neve, a kártyaszám, a kártya hátoldalán található háromjegyű biztonsági kód jelzi elsősorban. A bankkártya eme azonosítóinak jogellenes megszerzése történhet:
– adathalászat által (hamis banki oldalon történő adatközléssel, hamis tartalomközlő e-mailben – stb.),

[23] Europol: Internet Organised Cybercrime Threat Assessment 2016. 29-30. o. https://www.europol.europa.eu/iocta/2016/ [2018.05.20.] Europol: Internet Organised Cybercrime Threat Assessment 2017. 43-44. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 [2018.05.20.] https://www.investopedia.com/terms/c/cardnot-present-fraud.asp [2018.05.20.]

– korábbi tranzakciók esetében az adatok online kifürkészése által,
– korábbi tranzakciót követően a tisztességtelen dolgozók által,
– a bankkártyával fizikai kapcsolatba került személyek által.

A bankkártya használat bizalmasságát, titkosságát veszélyezteti a nyílt Wi-Fi vagy az általában a nem védett mobiltelefonok applikációinak a használata.

Az internet alvilágában a bankkártya adatoknak hatalmas értékük van. A kártyabirtokosnak nagy károkat okozhatnak. A bűnözők saját kényük-kedvük szerint költhetik a kártyabirtokos pénzét (megélhetésükre, kábítószerekre, hamis okmányokra, fegyverre, egy további bűncselekmény fizikai előkészületeire stb.).

A card-not-present csalás a Btk. 375.§-ba ütközik és az értékhatár megfelelő bekezdése szerint információs rendszer felhasználásával elkövetett csalásnak[24] minősül.

Érdemes továbbá megjegyezni, hogy bankkártyákkal kapcsolatos bűncselekmények tényleges károsultjai – s így sértettjei – a bankkártyákat kibocsátó pénzintézetek, azonban ők általában megtérítik egyből a bankkártya tulajdonosának a kárát, amennyiben nem volt neki felróható a bűncselekmény elkövetése.[25]

2.2.3. Az aukciós csalások, avagy átverések az árverésen

Az internetes aukciós oldalakon[26] a felhasználók licitálás útján tudnak vásárolni.[27] A licitálás lehetősége akkor nyílik meg az érdeklődő felhasználók előtt, ha azok regisztráltak az adott aukciós oldalra. Ha az online árverési oldalon regisztrálunk, egyrészt szerződéses jogviszonyba kerülünk az árverési oldal üzemeltetőjével, amely a regisztrációnk alapján az oldalon nyújtott szolgáltatásokhoz (aukción való részvétel, termékek árverésre való meghirdetése, a weboldal eléréséhez stb.) való hozzáférést biztosít. Az adott termék licitálásakor, és az árverés lezárását követően a termék eladójával kerülünk jogviszonyba. A szerződés nem – vagy hibás teljesítése miatt igényünket a termék eladójával szemben lehet érvényesíteni.

Az aukciós oldalakon, az eladó általában egyaránt megjelenhet a B2C és C2C relációjú kereskedelem. A vállalkozások, üzleti szféra számára több előnyt jelenthet, nevük, termékeik ismertté tehetők, az elfekvő, eladatlan készletek kiárusíthatók. Nyilván nagyobb tételben történő értékesítés nem igazán várható.

[24] Lásd ehhez: Kondorosi András: Az információs rendszer felhasználásával elkövetett csalás. Infokommunikáció és jog 2014/2. 73-75. o.

[25] BH 2004.11.452.; valamint Szabó Imre: Fizetek főúr, volt egy feketém – joghatóság, illetékesség a készpénz-helyettesítő fizetési eszközzel elkövetett bűncselekményeknél. Ügyészek Lapja 2015/6. 50.

[26] Lásd bővebben: Vincze Gabriella Anita: A digitális kor „gyermekei": az internetes aukciós oldalak és jogi problémáik. Magyar Jog 2016/7-8. 471-477. o.

[27] Bártfai Barnabás: Az internet lehetőségei. Budapest, BBS-Info.2008. 98-116.o.

Az eladó aukcióként felkínálja az értékesíteni kívánt tárgyat, amire az érdeklődő felhasználók licitálhatnak.

Az aukció éppúgy lehet sikertelen, mint sikeres. Sikertelen az aukció, ha az eladó visszavonja az áruját a licitálástól, vagy ha az eladó úgy gondolja, hogy a felkínált árak nem érik el az eladó által megkívánt árat, ami lehet az eredetinél akár kevesebb is, ha az eladó így dönt.

Sikeres a licitálás, ha a termék elkel az eladónak megfelel a vevő által felkínált ár. Általában a legjobb ajánlatot tevő vevő nyeri a licitálást. A sikeres aukciót követően az aukciós oldal üzemeltetője automatikus üzenetben közli a vevővel az eladó, az eladóval a vevő regisztrációkor megadott elérhetőségét. Az ügyletet a vevő és az eladó önállóan bonyolítja le.

A sikeres ügyletkötést követően az eladó jutalékot fizet az aukciós oldal üzemeltetőjének.

A sikeres ügyletkötést követően szükség van az eladónak a vevő, a vevőnek az eladó értékelésére. Ennek azért van jelentősége, hogy az értékelésből kitűnjön menynyire megbízható az adott partner, akár eladó, akár vevő oldalon.

A licitálásnak kétféle formája lehet:

– fixáras eladás, ebben az esetben alkudni sem lehet,
– meghatározott licitösszegről induló licitálás: a termék reális árához közeli vagy a licitálás során általában a reális ár körüli ár; vagy szándékosan eltérített, túl magas vagy túl alacsony ár (pl. a túl alacsony ár egyik speciális esete az 1 forintól induló ár).

A licitáló a kiválasztott tárgyat megtekintheti fényképen, elolvashatja róla a rövid ismertetőt, és ennek ismeretében licitálhat, órák, napok elteltével, akár többször is.

a) Csalás az aukció idején:

Nézzünk az árverésen történő átverések tipikus eseteit:

– Shill-csalás: ebben az esetben a licitálás során egy harmadik személy, egy hamis licitáns, vagy maga az eladó – hamis e-mail–címről, hamis azonosítóval – „tornássza fel" a licitárat. Kockázat nincs, hiszen, ha a shill-re marad az áru, nem történik semmi.
– Shield-csalás: ebben az esetben is a licitálás során egy harmadik személy, egy hamis licitáns, vagy maga a vevő – hamis e-mail–címről, hamis azonosítóval – „tornássza fel" a licitárat. Majd amikor a legmagasabb árral a shield magára marad, akkor alacsonyabb árért átengedi az igazi licitálóra.
– Mind a shill-, mind a shield-csalások szervezett elkövetést tételeznek fel.

b) Csalás az aukciót követően:[28]

A sikeres licitálást követően a nyertes vevő a vételár kiegyenlítését követően:

- Hamis, vagy (a licitálásra felkínált tárgyhoz képest) gyenge minőségű árut kap (Ptk. 6. könyv XXII. fejezet: A szerződésszegés általános szabályai).
- Egyáltalán nem kapja meg a kifizetett árut a vevő (csalás, Btk. 373.§).
- Bűncselekményből származó dolgot értékesített (orgazdaság, Btk. 379.§).

Az első két eset jórészt kivédhető, ha a licitáláson nyertes a postai utánvéttel történik az áru kifizetése, majd átvétele. Más kérdés, hogy az aukciós szabályzat megengedi-e az utánvétes áruvásárlást, vagy azonnal, bankkártyával történő kiegyenlítéséhez ragaszkodnak a licitálást szervezők.

Az orgazdaság a laikus számára is sokszor fel sem tűnik, fel sem tűnhet, fel nem tűnik. Esetleg a fizikai erőszakot mutató nyomsérülések, eredeti csomagolás hiánya (bár ez utóbbi a second-hand termékek esetében jellemző), akár a médiából is ismert (pl. körözött) tárgy, festmény, netán egy harmadik személy neve szerepel a tárgyakon stb. jelezhetik, hogy az áru vélhetően bűncselekményből származik.

c) Jutalék-csalás: az aukciónak és más second-hand értékesítési lehetőséget (tárhelyet, az eladó és vevők kölcsönös elérhetőségét stb.) biztosító vállalkozások a tranzakciókból meghatározott jutalékot szednek be, amely tevékenységük fenntarthatóságához járulnak hozzá.

Jutalék-csalás esetén az eladó vagy elhallgatja terméke sikeres értékesítését, vagy megpróbál „eltűnni" az aukciós – oldal látóköréből.

Az aukciós oldalak regisztrációval, majd ez alapján valós térbeli címre történő levél küldésével és válaszolási kötelezettséggel igyekeznek kiszűrni azokat, akik jutalék- vagy más csalási cselekményre használnák fel a C2C relációt.

d) Megtévesztő aukció adathalászat céljával:

Az aukcióra történő benevezés szokatlan formája az ún. 1 forintos aukció. A vevő 1 forintot köt ki a licitálás (vélhetően) elején, amikor az áruját megjeleníti a web-oldalon. Nem kétséges, kiváló reklámfogás, hiszen felkelti az érdeklődést és mintegy mézesmadzag az érdeklődő felhasználókban. Azt a téves képzetet keltheti, hogy a termék milyen olcsón beszerezhető, mert, ha történik is licitálás, még akkor is lehet, hogy nagyon olcsón megszerezhető az a termék.

Az átverés az árverésen a következő, bár úgy tűnik, hogy létrejön az alku (akár 1 forinton, akár egy másik összeggel) és ekkor az eladó megismeri a vevőt, megkapja a vevő elérhetőségét (e-mail cím, más azonosítók), majd az e-kereskedelem során

[28] Gercke, Marco: Understanding cybercrime: phenomena, challenges and legal response, Geneva, ITU. 2012. 30. o.

nem tiltott módon az eladó visszalép[29] (mert meggondolja magát, kitalál egy fals indokot stb.).

Az üzlet így nem jön létre, ám az eladó a vevő adatait már megszerezte.

A csalások formáiról tájékoztatást kapunk az aukciós oldalakon.

3. Esettanulmány: egy sikeresen felderített aukciós csalás

Lásunk egy sikeresen felderített összetett aukciós csalás bűncselekményt:[30] 2009. január feljelentés az egyik budapesti, kerületi rendőrkapitányságon: a sértett az aukciós online piactéren vásárolt két 25 ezer értékben vásárolt bőrdzsekit nem kapta meg. A hatósági az alábbi intézkedéseket rendelte el:

Megkeresés (1): az aukciós piactér felé:

– a gyanúsított(ak) regisztrációs adatai,
– belépési IP címek,
– eladott termékek, vásárlók (sértettek) adatai.

Megkeresés (2):

– az internetszolgáltató (hozzáférést biztosító szolgáltató) felé,
– 3 olyan bank felé, ahonnan az eladótól az ún. ellenőrző utalások érkeztek az online piactér számlájára.

Házkutatás a gyanúsítottnál:

– számítógép nem került elő (talán „készült" a gyanúsított?),
– előkerültek a 3 bank papírjain további 7 bank papírjai.
– Megkeresés (3): az online piactér felé a pénzutalások érkezhettek-e ezekből a bankokból?

Szembesítés azzal a sértettel, akitől a pénzt átvette: eredményes volt.

Az online piactér további felhasználóneveket azonosított, tehát több néven árultak 10 nevet felhasználó sikerült azonosítani.

Ugyanakkor gyanúsak voltak az eladóról szóló értékelések. Az egyik „vevő" többször több néven futó, de ugyanattól az „eladótól" vásárolt és pozitíve értékelte a tevékenységét (gyors, megbízható, korrekt, segítőkész stb.). A naplózott értékelések áttekintésekor: 33 pozitív értékelés érkezett két „vevőtől", ugyanazon, bár több néven szereplő „eladóról", pl. olyankor is, amikor a tranzakció még meg sem történt,

[29] 45/2014. (II. 26.) Korm. rendelet nem tiltja ezt a lehetőséget.

[30] Barta Sándor – Székely Gergely: Kézikönyv az online piactereken elkövetett visszaélések felderítéséhez. Budapest, Allegoup Kft. 2012. 8/1 – 8/7. o.

időben meg sem történhetett. Jutalék csalás gyanúja is felmerült: az eladó, a később „gyanúsított" nagy értékű számítógépeket árult a különböző online piactéren. Az eladó a regisztrációkor többek között a hamis neveken, hamis címeket adott meg. Minden név, nyilván nem véletlenül gyakori magyar név volt. Balszerencséjére vagy épp ellenkezőleg, hogy valódinak tűnjön az eladó, az egyik valós lakcímen valóban lakott egy felhasznált nevű személy, aki rendszeresen kapott felszólításokat, hogy az eladott terméke után a jutalékot fizesse be.

A címzett egy idő után megelégelte a felszólításokat és feljelentést tett a rendőrségen. A nyomozás során az IP-cím alapján azonosították az ismerősét, aki beismerő vallomást tett és így jutottak el a számítógépeket eladó gyanúsítotthoz. A nyomozás során az IP-cím alapján azonosították az ismerősét, aki beismerő vallomást tett és így jutottak el a számítógépeket eladó gyanúsítotthoz.

Illetékességi kérdések a büntetőeljárás során:

A csalás bűncselekménye kapcsán: a vételár kifizetése ellenére sem küldte az árut (telefont) az eladó. K-i bíróság (mint a sértett lakhelye) az egyik budapesti kerületi bírósághoz, mivel a szolgáltató székhelye, bankszámlája itt volt, a megtévesztő hirdetést itt adták fel. A kerületi bíróság az ügyet áttette Z-i bírósághoz, mivel a pénzutalás itt történt, hivatkozva a BH 2009. 317. döntésre, amely szerint csalás esetében a károkozó magatartás kifejtésének helye is megalapozhatja a bíróság illetékességét. A BH 2011. 332 sz. ítélet szerint „a megtévesztés akkor történt, amikor a sértett az interneten szembesült a vádlott megtévesztő szándékkal internetre feltett és azáltal közvetített eladási ajánlatával. Ehhez képest a károkozó magatartás kifejtése (pénzátutalás) és az eredmény bekövetkezte is értelemszerűen a sértett lakóhelyén történt. Ekként valamennyi esetben ez az elkövetés helye."

Kriminálmetodikai szempontból „állatorvosi ló" ez az eset:

- több sértett lehet; üzletszerűség gyanúja,
- sértettek az ország különböző pontjain lakhatnak,
- megkeresések szükségesek: az aukciós oldalt üzemeltető felé; pénzintézet(ek); a hozzáférést biztosító szolgáltatók felé; a mobilszolgáltatók felé (regisztrációs adat); vagy más irányba is pl. posta (kézbesítés adataira vonatkozóan).
- többféle (egymással általában összefüggő) bűncselekményre kell figyelni; csalás, okirati
- bűncselekmények, gondatlan pénzmosás, orgazdaság stb.
- több bűncselekmény valószínűsíti a több elkövetőt.

Nyílt forrású információgyűjtés (OSINT) fontossága az interneten[31]:

– Az elkövető(k) irányában: A regisztrációkor megadott adatok ellenőrzése: név, lakcím, telefonszám, e-mail cím stb. A vásárlási értesítőben megadott adatok: név, lakcím, bankszámla szám, telefonszám stb. Az ellenőrző utalások adatai: számlaszám, utalást teljesítő neve stb.
– Tanúk, sértettek irányában: az eladóval történő kapcsolattartás formáira: telefonszámok, e-mail címek, posta leveleken, levelezőlapokon szereplő címek, személyes találkozások stb.
– Milyen számlára, milyen névre, mikor, mennyi pénzt utaltak a bankok.

Egyéb, a nyomozás során felmerült adatok ellenőrzése:

– a megkeresésekre érkezett adatok, információk ellenőrzése, azok segítségével további
– megkeresések, ellenőrzések, sértettek, tanúk stb.
– Facebookon, Twitteren: kép, név, cím, e-mail, ismerősök, baráti kör, érdeklődési köre,
– aktuális fizikai kinézete, tartózkodás helye, gépkocsija, szórakozási szokásai, törzshelyei stb.
– Google: mit csinál, mit keres, mit akar venni, hová akar utazni, szórakozni menni stb.

Felhasznált Irodalom

Ambrus István – Deák Zoltán: Súlyponti kérdések a bankkártyával kapcsolatos bűncselekmények köréből. Belügyi Szemle 2011/2.

Barta Sándor – Székely Gergely: Kézikönyv az online piactereken elkövetett visszaélések felderítéséhez. Budapest, Allegoup Kft. 2012.

Bártfai Barnabás: Az internet lehetőségei. Budapest, BBS-Info. 2008.

Clough, Jonathan: Principles of cybercrime. Second Edition. Cambridge University Press, 2015.

Erdősy Emil – Földvári József – Tóth Mihály: Magyar Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2004.

Europol: Internet Organised Cybercrime Threat Assessment 2016.

Europol: Internet Organised Cybercrime Threat Assessment 2017.

[31] Lásd Herédi István: Nyílt forrású adatgyűjtés az interneten. Belügyi Szemle 2018/7-8. 106-116. o.

GERCKE, Marco: Understanding cybercrime: phenomena, challenges and legal response, Geneva, ITU. 2012.
GOODMAN, Marc: Future Crimes. London, Transworld Publishers, Corgi Book, 2016.
GYARAKI Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012.
HERÉDI István: Nyílt forrású adatgyűjtés az interneten. Belügyi Szemle 2018/7-8.
KONDOROSI András: Az információs rendszer felhasználásával elkövetett csalás. Infokommunikáció és jog 2014/2.
KONDRICSZ Péter – TÍMÁR András: Az elektronikus kereskedelem jogi kérdései. Budapest, KJK-Kerszöv. Jogi és Üzleti Kiadó, 2000.
MEZEI Kitti – TÓTH Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós-Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017.
MEZEI Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1.
NAGY Richárd: A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései. Belügyi Szemle 2018/7-8.
NAGY Zoltán András: Bűncselekmények, számítógépes környezetben. Budapest, Ad-Librum, 2009.
NAGY Zoltán András: Sport és büntetőjog. Pécs, Kódex Nyomda, 2014.
NAGY Zoltán: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1. 1992/1.
SENKER, Cath: Cybercrime and the Darknet. London, Arcturus Holdings Ltd., 2017.
SIMON Béla: A rendőrségi állomány felkészültsége a kiberbűnözésre. Hadtudományi Szemle 2018/1.
SZABÓ Imre: Fizetek főúr, volt egy feketém – joghatóság, illetékesség a készpénz-helyettesítő fizetési eszközzel elkövetett bűncselekményeknél. Ügyészek Lapja 2015/6.
SZATHMÁRY Zoltán: A hamis termékek forgalmazásával elkövetett iparjogvédelmi jogok bizonyításának nehézségei. Ügyészek Lapja 2015/2.
TÓTH Mihály: Fogyasztók megtévesztése. In: Tóth Mihály – Nagy Zoltán (szerk.): Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2014.
TÓTH Mihály: Rossz minőségű termék forgalomba hozatala. In: Tóth Mihály – Nagy Zoltán (szerk.): Büntetőjog – Különös Rész. Budapest, Osiris Kiadó, 2014.
TÓTH Mihály: Gazdasági bűnözés és bűncselekmények. Budapest, KJK-Kerszöv., 2002.
VINCZE Gabriella Anita: A digitális kor „gyermekei": az internetes aukciós oldalak és jogi problémáik. Magyar Jog 2016/7-8.

SIMON BÉLA

A KRIPTOVALUTÁK ÉS A KAPCSOLÓDÓ RENDÉSZETI KIHÍVÁSOK

1. Bevezetés

Az emberi társadalom számos funkciót, eljárást és intézményt fejlesztett ki a saját maga és tagjai védelmére. Kijelenthetjük, hogy ezek a megoldások mindig akkor hasznosak, ha a kialakításuk, fenntartásuk során felhasznált erőforrások kisebbek, mint a védendő társadalmi érték, melynek megóvására hivatottak.

A helyes döntést egy mérleg két serpenyőjét vizsgálva találjuk: az egyik oldalon a védekezés költsége, a másik oldalon pedig a veszélyeztetett érték található. Utóbbi serpenyő távolságát a felfüggesztéstől a kár bekövetkezésének valósínűsége határozza meg. A súlyok és arányok azonban nehezen meghatározhatók. Ebben az összefüggésben vizsgáltuk a kriptovaluták problémakörét. Mekkora érték? Mekkora veszély? Mekkora intézkedéseket kell tenni a lehetséges problémákra?

Vajon egy hirtelen felkapott téma a kriptovaluták okozta új problémák, és felesleges vele foglalkozni, vagy valóban forradalmasíthatja a pénzügyi rendszert és akár befolyásolhatja a társadalom működését?[1]?

A cél tehát a kriptovaluták közérthető bemutatásán keresztül kiemelni néhány aspektust, amelyre a rendészeti szerveknek választ kell adni.

2. Mi is a kriptovaluta?

Számos definícióval találkozhatunk e fogalom körül határolása során. Az alábbiakban megkísérelem olyan kis mértékben informatikai szakkifejezéseket használva leírni a működést, ami a továbbiak megértéséhez feltétlenül szükséges.

Gyakran a kriptovalutákat és az elektronikus pénzt egymás szinonimájaként használják. A két fogalom azonban élesen elválik egymástól. Az elektronikus pénz a jegy-

[1] Korábban az internetről sem feltételezték, hogy ilyen átütő hatása lesz a mindennapjainkra, továbbá ha nem is megyünk vissza a távoli múltba, akkor a Facebook is egy jelentéktelen internetes oldalnak tűnt sokak számára.

bankok által kibocsátott pénz egyik – dematerializált – megjelenési formája, de azzal azonosjoghatásokkal.[2] A kriptovaluták esetében azonban nem beszélhetünk jegybanki, vagy állami elfogadásról[3] – azokat mindenki önként elfogadhatja olyan értéken, amennyiért akarja: csak a kereslet és kínálat határozza meg az árfolyamot, így a monetáris politika eszközrendszere sem működhet. A kriptovalutákat – bár pénz funkcióval bírnak – nem nevezhetjük törvényes fizetőeszköznek, azaz pénznek.

Sok esetben a virtuális valutát és a kriptovalutákat egymás szinonimájaként használják. A virtuális valuta sokkal tágabb kör. A virtuális valuták digitális formában megjelenő, de állami szabályozás nélküli valuták[4]. A kriptovaluták ezen belül képeznek egy csoportot, amelyeknek az a sajátos ismérvük, hogy kriptográfiai hitelesítő folyamatok – tipikusan blokklánc technológia – által lehet őket létrehozni.

Fontos leszögezni, hogy a bitcoin[5] csak egy a több ezer kriptovalutából, de vitathatatlanul a legnagyobb hatású. A sikerén felbuzdulva sok csoport írt számítógépes programot, amely kriptovaluták előállítását teszi lehetővé, és ezek közül vannak, amelyek szolgáltatásaikban, felhasználhatóságukban felülmúlják a bitcoint, de jelenleg ez a kriptovaluta a legelterjedtebb és ez rendelkezik a legnagyobb bizalommal a felhasználók részéről. A lényegesebb kriptovaluták különféle internetes oldalakon ismerhetők meg.[6]

1. *táblázat: Pénz mátrix*

A pénz mátrix[7]			
Jogi státusza szerint	Szabályozatlan	egyes helyi valuták	Virtuális valuták
	Szabályozott	Bankjegyek és érmék	elektronikus pénz
			számlapénz (letét)
		fizikai	digitális
		megjelenési forma	

[2] A hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény 6. § 16. pontjában megfogalmazottak szerint.

[3] Az MNB már 2014. évben rendkívül kockázatosnak ítélte a bitcoint (300-1000 USD közti árfolyamsávban). https://www.mnb.hu/archivum/Felugyelet/root/fooldal/topmenu/sajto/sajtokozlemenyek/bitcoin_kozl [2018.04.30] Azonban vannak olyan törekvések, ahol önkormányzatok elfogadják, vagy a blokklánc technológiát állami célokra használják. https://coincolors.co/2017/09/12/dubajban-lakast-svajcban-adot-lehet-fizetni-bitcoinnal/ [2018.04.30.]

[4] Ide tartoznak különféle számítógépes játékokban gyűjthető „érmék" is még akkor is, ha azokat valamilyen formában rendes pénzre lehet váltani.

[5] Szokásos rövidítése: BTC.

[6] Ilyen például a https://coinranking.com/ és a https://coinmarketcap.com/.

[7] https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [2018.05.26.]

A témánk szempontjából leglényegesebb közös jellemzőik:
– központi adminisztráció/felügyelet nélküli rendszer
– alkalmas a pénz funkcióinak ellátására.

Nakamoto Satoshi[8] feltaláló célja a 2007-08-as gazdasági válság időszakában az volt, hogy kialakítson egy decentralizált és önmagát fenntartó pénzügyi rendszert, amely sokkal hatékonyabb és olcsóbb, mint a jelenlegi bankrendszer. A megoldást egy olyan szisztéma kidolgozásában látta, amely nem a közvetítőbe helyezett bizalomra épít, hanem kriptográfiára és elemi számítások sokaságára bízza a tranzakciók validálását, egy peer-to-peer hálózaton. Ez mindaddig biztonságot nyújt az egész rendszernek, amíg a rendszert becsületesen használni kívánók összessége több számítási kapacitással bír, mint bármely a rendszer kijátszására apelláló személy vagy csoport a hálózatban.[9]

Ahhoz, hogy ez a rendszer kialakulhasson, először motiválni kell a lehetséges szereplőket, hogy belépjenek. Ezt a motivációt a bányászat által megtermelt kriptovaluta jelenti. Ha már egyszer kialakult, akkor akár a tranzakciós díjakból is fenntartható a működés.

Ahhoz, hogy valami pénzként funkcionáljon – szükséges egy központi elem, amelyben a felek megbíznak. A bankrendszerben, a nemzeti valutákban ezt a bizalmat többek között:
– a pénzintézeteket szabályozó jogi normák,
– a kapcsolódó intézmények és
– az állami kezességvállalás tartják fenn.[10]

A kriptovaluták esetében a bizalom legfontosabb – és talán egyetlen – alapja az a matematikai algoritmus, amely az adott kriptovalutát létrehozta. Ez egy bonyolult egyenlet, melyhez összetett számítási folyamatokon keresztül véges számú megoldás társul. A bitcoin esetében ez közel 21 millió. Aki kriptovalutát bányászik, az a számítógépének teljesítményét az adott kriptovalutához kapcsolódó matematikai feladvány számítására áldozza.[11] Ennek ellentételezéseként időszakonként kriptova-

[8] Ezen a néven kerültek publikálásra a bitcoin rendszer alapvetései, de máig nem ismert az a konkrét személy vagy csoport, aki ezt kidolgozta.

[9] Bakó Tamás: Bitcoin hálózatok elemzése (Diplomamunka). Eötvös Loránd Tudományegyetem, Természettudományi Kar, Matematikai Intézet 2015. 7. o.

[10] Bármelyik bizalmi alapként működő elem gyengülése a nemzeti valuta gyengülését is eredményezi.

[11] Az önálló bányászat nem jellemző. Gyakrabban csoportokba (pool) gyűjtik a bányász gépeket és a közös bitcoint felosztják egymás közt a munkájuk arányában. Ilyen bányász pool-ok például a következők: F2Pool, KnCMinerB, AntPool, MaxBTC, BitFury/SEGWIT stb.

lutákat kap[12] a sok egymással mellérendelő viszonyban álló számítógépből felépülő nagy internetes hálózatból[13].

Az, hogy bizonyos javakból korlátozott mennyiség áll rendelkezésre, az mindenképpen árfelhajtó hatású.[14] A korlátozott számú előállíthatóság minden kriptovaluta esetében érvényes.

Ahhoz, hogy egy digitális jel önmagában értéket képviseljen, ahhoz meg kell szüntetni egyik legfontosabb tulajdonságát, azt, hogy a róla készült másolat vele teljesen azonos[15]. A kriptovaluták esetében ezt úgy oldják meg, hogy ezeket a digitális jeleket egymáshoz fűzik és egy nagy egyenrangú internetes hálózatban nagyon sok számítógép egymással párhuzamosan ugyanazon egymáshoz fűzött adatot fűzi tovább[16]. Ez a blokklánc. A blokklánc megmutatja, hogy ebben az adatfolyamban az „egyenlet melyik megoldása" melyik megfejtőnél van, vagy azt kinek adta tovább.

Nagyon fontos, hogy a kriptovaluták jellemzően feloszthatók. A bitcoin esetében ez nyolc tizedesig lehetséges 1 bitcoin = 100.000.000 satoshi. Tehát amint a forintnak a fillér (volt) a két tizedesig tartó váltópénze, úgy a bitcoinnak a satoshi a 8 tizedesig tartó váltópénze.

Az előbbi példánál maradva tehát ha valaki egy hagyományos számítógéppel elkezd bitcoint bányászni, akkor annak ellentételezéseként nem csak egész bitcoint kaphat, hanem ennek tört részét is. Vásárolni is lehet tört bitcoint is, sőt az jellemző.[17]

Az adott kriptovalutát életben tartó blokklánc tehát folyamatosan nagyszámú számítógépen elérhető az interneten, ami egy peer-to-peer (P2P) hálózat, ami egészen más, mint az ügyfél-szerver megoldás. A peer-to-peer olyan, mint egy pletykahálózat, ahol mindenki elmondja néhány embernek a híreket (új tranzakciókról és új blokkokról), és végül az üzenet mindenki számára elérhető lesz a hálózatban.

[12] A kriptovalutát sem úgy kell elképzelni, hogy az egy egyedi karakterlánc, vagy kódsor, hanem az egy nagy főkönyvben egy bejegyzés, hogy egyik, vagy másik felhasználónak van belőle 2, vagy 0,0012 darab.

[13] Maga a matematikai feladvány és annak megoldása a kriptovaluták működésének megértéséhez nem is fontos. Sőt maga a feladvány sem fontos a témánk szempontjából és a kriptovaluta fejlesztőknél is inkább az volt az egyik legfontosabb cél, hogy az informatikai eszközökkel erőforrásigényesen lehessen csak megoldani, azaz ne lehessen egy egyszerű számítógéppel megtalálni az összes megoldást.

[14] A fordítottja is igaz, hisz ha sikerülne ólomból aranyat előállítani, vagy könnyen lehetne tiszta gyémántkristályokat előállítani, akkor értékük hatalmasat zuhanna.

[15] Ha egy szöveges fájlról, képről, számítógépes programról, bekódolt merevlemezről bitről bitre készítek egy másolatot, akkor azok teljesen ugyanolyanok lesznek.

[16] A folyamatosan és párhuzamosan fűzött blokkláncban benne van, hogy melyik tárca mikor és mennyi kriptovalutát kapott és azt megtartotta, vagy tovább transzferálta.

[17] Bővebben: https://bitinfocharts.com/bitcoin/explorer/ ahol az is látható, hogy milyen tranzakciók kerülnek egy blokkba, azok mennyi időnként jönnek létre.

Ez ellentétben áll a hagyományosan használt ügyfél-szerver hálózattal, ahol a főnök az alárendelteknek tájékoztatja a híreket, és a főnök egy központi referenciapont és potenciális veszélyforrás: sérülésével megszűnik az információáramlás.[18]

A kriptovaluták felhasználhatóságát Satoshi Nakamoto is leginkább a bankrendszer kiváltásában látta, mivel olcsóbban tud működni, mint a jelenlegi bakrendszer. Azt is látnunk kell azonban, hogy e rendszer működése is erőforrás igényes (informatikai eszközök fejlesztése és működtetése leginkább) és egy kriptovaluta egység előállítása is bizonyos egységű egyéb javak felhasználásával történik[19]. A kriptovaluták akkor tudnak költséghatékony alternatívái lenni a jelenlegi pénzügyi rendszernek, ha egy adott egységnyi pénz funkciót (pl: x érték transzferálása két fél közt) sokkal kedvezőbb költségekkel tudnak megvalósítani.[20]

A kriptovaluták ún. tárcákban helyezkednek el. Ezek a tárcák a blokkláncba fűzve szintén digitális adatok. A tárcák is teljesen egyedi azonosítóval rendelkeznek. A tárcában való elhelyezést nem úgy kell érteni, hogy egy kódsor megjelenik egy mappában és minél több kriptovalutánk van, annál nagyobb lesz az adott fájl. E tekintetben sokkal inkább hasonlít a rendszer a banki számlapénzre, vagy az értékpapírszámlákra: amikor a bankszámlánkról utalás történik, akkor nem adott sorszámú bankjegyek indulnak el a célszámlára, hanem van egy egyenleg és a számlatulajdonos utasítja a számlavezetőjét, hogy számláját annyival terhelje, amennyivel a célzott számlán jóváírást teljesít.

A kriptovaluták esetében tehát ez a blokklánc egy főkönyv, melyben folyamatosan szerepelnek a létrejövő kriptovaluták és azoknak az aktuális helye és mozgása is nyomon követhető. 2018 júniusáig a teljes bitcoin blokklánc mérete (adatbázis indexekkel) meghaladta a 15 GB-ot és a tárolt tranzakciók száma a 320 milliót.[21]

[18] https://bitsonblocks.net/2015/09/01/a-gentle-introduction-to-bitcoin/ [2018.05.25.]

[19] Hasonlóan a jelenlegi pénzeknél nem csak a pénzjegynyomda egy bankjegyre eső előállítási költségét kell figyelembe venni, hanem az egy egységnyi pénznek a pénz funkció betöltéséhez szükséges összes költségét (pld: egy átutalásnál a bank épületének, informatikai infrastruktúrájának arra eső költségét).

[20] Itt ismételten figyelembe kell venni a kriptovaluta előállítási kötségén felül a rendszer fenntartásának, üzemeltetésének költségét az x egységnyi értékre vonatkozóan. Persze ezt a képletet a megbízhatóság és a kényelmi funkciók erősen árnyalják.

[21] https://blockchain.info/hu/charts/n-transactions-total?timespan=all [2018.06.01.] Bővebben: https://blockchain.info/charts; E könyvrészlet írásakor a bitcoin esetében ez a tiszta blokklánc 170Mb – https://blockchain.info/charts/blocks-size [2018.06.05.]

3. Mi a kriptovaluta tárca?

Bűnüldözési szempontból tehát nagyon fontos, hogy a nyomozás érdekében, vagy akár csak a polgárjogi igény érvényre juttatása miatt szükséges lefoglalni a kriptovalutákat, vagyis leginkább átvenni a hatalmat az érintett mennyiségű kriptovaluta felett. Ehhez szükséges ismernünk ezen javaknak a fellelhetőségi helyét – azaz a tárcákat (wallet).

A bányászattal nem foglalkozó személy, aki szeretne kriptovalutát tulajdonolni – mindenképpen egy tárca alkalmazást kell, hogy használjon[22] (telefonon, számítógépen, tableten stb., szinte bármilyen operációs rendszeren).

A tárca alkalmazás legfontosabb funkciói:

– létrehozza tulajdonképpen a tárcát, ami a lehetőséget biztosítja a blokklánchoz való kapcsolódásra,
– létrehoz a tárcában publikus kulcsokat (public key – amit a számlaszámhoz hasonlatosnak tekinthetünk) és azokhoz illő privát kulcsokat (private key – amit a számlához tartozó jelszóként értékelhetünk),
– kapcsolatot tud kiépíteni a kriptovaluta blokkláncát üzemeltető internetes hálózattal és annak üzenetet tud küldeni és onnan üzeneteket tud megjeleníteni a kezdeményezett tranzakciókról.[23]

A kriptovaluta tárcánk nem tárolja a megvásárolt, vagy kibányászott bitcoinokat, csak a számlaszámot (ez a publikus kulcs) és egy jelszót (ez a privát kulcs). Ezen a kulcspárok esetében nagyon fontos, hogy tulajdonképpen egyediek.

A bitcoin-ban egy privát kulcs 256 bites szám,[24] amely többféleképpen is megjelenhet. Egy hexadecimális (azaz 16-os számrendszerben felírt) 256 bites számot 64 karakterben lehet leírni, mely karakterek tartományai 0-9 vagy A-F.[25] A privát kulcs tehát egy nagyon hosszú szám-és betűsor, melyből a tárca alkalmazás nyeri a felhatalmazást arra, hogy a kriptovaluták feletti rendelkezéseket végrehajtsa, azaz

[22] Még a blokklánc üzemeltetésében és fejlesztésében részt vevő bányászattal foglalkozó számítógépeknek is a munkájuk gyümölcseként kapott kriptovalutát is tárcákban kell elhelyezni.

[23] Számos további funkció is kapcsolódhat a tárca applikációhoz. Például jelszavas védelem az egész tárcára, a kriptovalutákkal foglalkozó tőzsdék adatainak megjelenítése stb.

[24] Azaz 256 karakteren 0, vagy 1 – így 2 a 256. hatványon verziót vehet fel – ez meglehetősen nagy variációt ad: összesen: 115.792 duodecillió 089.237 undecillió 316.195 decillió 423.570 nonillió 985.008 oktillió 687.907 szeptillió 853.269 szextillió 984 kvintilliárd 665 kvintillió 640 kvadrilliárd 564 kvadrillió 039 trilliárd 457 trillió 584 billiárd 007 billió 913 milliárd 129 millió 639 ezer 936 lehetséges variáció, ha a 10es számrendszert használjuk.

[25] Például: 5JBvhsfA5JesmcVTGNrb3gkHGgv67hwY5hUws1Pmdj65jRM9nPF

például elküldje azokat egy másik tárcába. Fontos, hogy privát kulcsból egy matematikai művelettel kialakítható a publikus kulcs,[26] de ez irreverzibilis folyamat. A publikus kulcs jellemzően 33, vagy 34 karakter hosszú és alfanumerikus jegyekből áll.[27] Tipikusan 1-es, vagy 3-as számjeggyel kezdődik.[28]Tehát aki ismeri a privát kulcsot, kontrollálja a tárca tartalmát.

3.1. Kriptovaluta tárca típusok

A kriptovalutákhoz kapcsolódó kulcspár tárolásának számos formája alakult ki. Nem szükséges, hogy ez egy digitális kódsor legyen, hanem akár papírlapra írva, vagy IT eszközök által könnyen feldolgozható módon (pld kinyomtatott QR kód) is tárolhatók, vagy akár meg is jegyezhetők (vagy egy memorizált dalszövegből, verssorból legenerálhatók). A felhasználói igények, az informatikai szolgáltatók, illetve az informatikai eszközök lehetőségeinek csomópontjában az alábbi tárca típusok alakultak ki:

A csoportosítás a csomópont teljessége alapján:

a) Teljes csomópont (tartalmazza a teljes blokkláncot);
b) Könnyű (light)tárca (nem tárolják a blockchain teljes másolatát).

Csoportosítás az online lét alapján:

a) A forró tárca („hot wallet") (folyamatosan az internethez kapcsolódik);
   aa) Web alapú tárcák – egy szolgáltató webes felületén elérhető;
   ab) Desktop tárcák – a privát kulcsot a számítógépen tárolják;
   ac) Mobil tárcák – a privát kulcsot a mobiltelefonon tárolják;
b) Hideg tárolás avagy offline kriptovaluta tárca;
   ba) Papír alapú tárcák – kinyomtatott kulcspárok;
   bb) Hardver tárca – speciális pendrive-hoz hasonló eszközök-

További tárca csoportok:

a) Brain avagy „agy" tárca – a kulcsok, vagy a kulcsok alapjául szolgáló szavakat a felhasználó megjegyezi;
b) Többszörös identifikációs kriptovaluta tárca[29] – több privát kulcs egyidejű használata szükséges a tranzakció lebonyolításához. A „multisig" tárca csak

[26] Bővebben: https://medium.com/@karthikmargabandu7/public-keys-private-keys-and-bitcoin-address-bf26125addf7 vagy https://bitcoin.hu/archivum/bevezeto/hogyan-mukodik-a-bitcoin/a-bitcoin-cimek-technikai-hattere/

[27] Az elgépelések, félreértések elkerülése érdekében a Base58Check egyéni kódolási képletet használja, amely nem használja a 0, a O, az I és az l karaktereket és tartalmaz magában ellenőrző karaktereket is a pontatlanság elkerülése érdekében.

[28] Például: 1FsGty1hk4HoXAVEXGV73GeVdXnec8SjUt

[29] Franco, Pedro: Understanding Bitcoin: Cryptography, engineering and economics. Wiley, 2015. 84. o.

akkor engedélyezi a kriptovaluták küldését, ha azt elegendő számú privát kulccsal igazolást kap – az előre meghatározott kulcsok közül. Ez utóbbi tárca típus a hatósági felügyelet alatt álló kriptovaluták tárolására is alkalmas, hiszen így jelentősen csökkenthető annak az esélye, hogy a lefoglalt kriptopénzekkel a hatóság bármely tagja önállóan sajátjaként rendelkezzen.

4. A kriptovaluták további ismérvei

A kriptovaluták és a hozzájuk kapcsolódó tárcák ismertetése után tehát két fontos tulajdonságukat kell kiemelni: korlátozott számban érhetők el és egy adott pillanatban csak egy helyen/egy tárcában létezhetnek.

Ha ezen tulajdonságok bármelyike sérül, akkor kriptovalutába vetett bizalom azonnal megrendül és az a kriptovaluta végét jelentené, de ilyenre eddig az ismert kriptovalutáknál még nem került sor.

Az elmúlt időszakban a kriptovaluták és a létező legális pénzügyi rendszer közé számos innovatív kapcsolatot létesítettek. Van olyan szolgáltatás, ahol ingyenesen lehet bankszámlát nyitni és az arra utalt, vagy bankkártyával feltöltött összegből bitcoint vásárolni. Lehetséges teljesen ingyenesen Visa kártyát igényelni[30] és a hozzá kapcsolódó telefonos applikációval folyamatosan lehet a kriptovalutánkat visszaváltani és devizautalásokat, vagy kártyás fizetéseket teljesíteni.[31] Vannak olyan szolgáltatások is, amelyek lehetővé teszik, hogy egy Visa bankkártya mögött elhelyezett betéti számlához egy bitcoin tárcát ad a szolgáltató és a bankkártyás fizetés mellet a rendszer átváltja aktuális árfolyamon a bitcoint és teljesíti a kártyás fizetést[32].

Mindezen szolgáltatások azonban messze nem olyan népszerűek, mint a hagyományos kártyás fizetési eljárások és a feltörekvő cégek sokszor jelentős díjat számítanak fel a szolgáltatásaikért. Valahol a kriptovaluta eladási és vételi ára közti különbözettel, valahol a kriptovaluta transzferálásának költségével.[33]

A tendencia azonban jól látható: a hagyományos – és a felhasználók számára könnyen kezelhető – pénzügyi szolgáltatások közé bekerülnek a kriptovaluták is

[30] Jelen tanulmányban számos szolgáltatás kerül említésre, de ezek nem a promótálást szolgálják, hanem csupán a szolgáltatások széles körére kívánnak példákat bemutatni.

[31] Ilyen például a revolut.com, – viszont a vásárolt bitcoin nem egy általunk is ismert tárcában jelenik meg. Az ügyfél csak az egyenleget ismeri és a kriptovalutát nem is transzferálhatja. E szolgáltatásban a bitcoin kincsképző pénz funkciót lát el.

[32] Ilyen például a SpectroCoin VISA Debit Card, vagy www.coinizy.com/; coinsbank.com/; www.bitwala.io/; xapo.com/; cryptopay.me; wirexapp.com; www.advcash.com/en/.

[33] Nem ritka az 1%, vagy 0,0025BTC költségként megjelölve (a kettőből a magasabb)

olyan módon akár, hogy a felhasználóknak semmilyen ismerete nincs a blokklánc technológiáról.

A kriptovaluták egyik fő értéke, hogy gyorsan, szinte azonnal teljesedésbe mennek a tranzakciók. A valóság azonban nem teljesen ezt igazolja. A bitcoin esetében az az időszak, amikorra a tranzakció véglegesen a blokkláncra kerül 2018. évben 5-10 perc, de jelentős forgalom esetén volt, amikor ez 29[34] percig tartott. A rendszer leterheltségétől és a felajánlott díjtól függ, hogy mennyi idő alatt kerül fel a blokkláncra a tranzakció. Ez a múltban extrém esetben akár 16 óra is volt.[35]

Egy kutató cég, – amely a különböző kriptovaluták piacán végzett tevékenységeket vizsgálja, – becslése szerint 2,78 és 3,79 millió közötti, vagyis az összes bitcoin 17-23 százaléka elveszett. Számos módon lehet elveszíteni a bitcoint. Lehetséges, egyszerűen elveszíteni a privát kulcsot vagy az azt tároló eszközt, [36] de hibás programok futtatása, vagy szoftverhibák is vezethetnek ilyen eredményre. A bányászat során számos lehetőség van az érmék elveszítésére: például a díjak lehívásának elmulasztása. Az is a kriptovaluták végleges elégetését jelenti, ha valaki olyan tárcára utal, amelyhez nincsen senkinek hozzáférése.[37]

A nyomozóhatóságok számára is lehetőség a kriptovaluták tranzakciós listájának – főkönyvének – értékelése, elemzése. A blokklácban szerepelnek az adatok. Vannak publikus oldalak – legfőképpen a bitcoin-ra[38] – amelyekből könnyen és felhasználóbarát módon lehet információt gyűjteni. Ilyenek a https://explorer.bitcoin.com https://blockchain.info/hu https://blockexplorer.com,[39] ahol a tárcák publikus címeinek ismeretében megnézhetjük a tranzakciók listáját, az összes érkezett bitcoin mennyiségét és az aktuális egyenleget.[40]

Nagyon fontos kiemelni azonban, hogy az anonimitás csupán viszonylagos a kriptovaluták világában; bár az adott címek használói alapvetően teljesen ismeretlenek, azonban a címek közötti utalások iránya, azok ideje és nagysága minden-

[34] Bővebben: https://blockchain.info/hu/charts/median-confirmation-time?timespan=all

[35] Buchko, Steven: How long do bitcoin transactions take? https://coincentral.com/how-long-do-bitcoin-transfers-take/ [2018.06.02.]

[36] Ennek egyik leghíresebb esetét James Howells, a londoni informatikus, aki elvesztette a 7500 bitcoint, vagyis körülbelül 56 millió dollárt, amikor laptopját 2013-ban eldobták. Elon Musk is tett olyan nyilatkozatot, hogy elfelejtette, hogyan érheti el digitális érméinek egy részét.

[37] Matsakis, Louise: How Wired lost $100,000 in bitcoin, https://www.wired.com/story/wired-lost-bitcoin/?mbid=BottomRelatedStories_Sections_5 [2018.06.02.]

[38] A második legértékesebb kriptovaluta az Ethereum elérhető a www.etherscan.io oldalon.

[39] Nem csak a bitcoin blokklánca tekinthető meg: https://etherscan.io/ https://chainz.cryptoid.info/.

[40] Megtekinthetjük, hogy például a WikiLeaks tárcájára (más forrásból megismert tárca nyilvános kulcsa: 1BTCorgHwCg6u2YSAWKgS17qUad6kHmtQW) 2018. június 1-ig több mint 5884 BTC érkezett, de kevesebb, mint 1 található rajta.

ki számára látható. Ezért is nevezik a rendszert sokszor inkább pszeudonimnak,[41] hiszen ha a tranzakciók láncolatában egyetlen címet is sikerül valamilyen módon valós személyhez kötni, onnantól fogva az egész utalástörténete (ideértve a jövőbeli tranzakcióit is) ismertté válik a nyomozó hatóság előtt.[42]

A legújabb tendencia szerint azonban a tárcákat az anonimítás fokozása érdekében tovább fejlesztették. Van olyan mobiltárca, amelyik mindössze 10 bitcoin címet cserélget véletlenszerűen (mindenkinek egyénileg a saját tárcájában), míg más tárcák minden egyes tranzakcióhoz egy teljesen új bitcoin címet generálnak.

A nyomozások során a kriptovaluták globális jellege folytán azonban a blokkláncban szereplő és a hatóságok számára ismert személy ugyanúgy lehet az utca végén, ahogy a föld másik sarkában. A kriptovalutákat a felhasználók egyre inkább a mindennapi ügyletekhez is használják (földrajzi helyhez kötődő áru vásárlása, vagy szolgáltatás igénybevétele),[43] ezen túlmenően pedig egyre több kriptovaluta tárcakezelő szolgáltató csak olyan ügyfél tranzakcióit hajtja végre, aki email címes azonosításon kívül okmányaival igazolta magát, vagy legalább telefonos azonosítást is megvalósított, így gátolva a pénzmosás jellegű bűncselekményekben való közreműködést.

A minden egyes utaláshoz egyedi kulcspár létrehozatalát megelőzően is beindítottak olyan szolgáltatásokat a kriptovalutával foglalkozó személyek, amelyeknek az a célja, hogy a kriptovaluta eredetét a blokkláncban követhetetlenné tegye. Ezt olyan módon valósítják meg, hogy egy-egy nagyobb mennyiségű tranzakcióban érintett kriptovalutát egy tárcába transzferálják, majd – némi szolgáltatási díjért cserébe – a nagy közös összegből utalják tovább a kriptovalutákat akár kisebb összegekben is – így érve el az összegek követhetetlenségét.

Fontos a nyomozóhatóságok és a titkosszolgálatok hatékony megelőző, felderítő jellegű tevékenysége.[44] Ahogy egyes anonimizáló proxy szervert, vagy TOR hálózat exit node-ot is (minden bizonnyal) titkosszolgálatok üzemeltetnek, úgy érdemes ezeket a szolgáltatásokat is létrehozni az abból megszerezhető információk érdekében.

---

[41] Lásd MÖSER, Malte: Anonymity of Bitcoin Transactions. 2013. 1. o. https://www.wi.uni-muenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf [2018.04.24]

[42] HALÁSZ Viktor: Kriptovaluták a bűnüldözésben – új kihívások és lehetséges válaszok (Diplomamunka). NKE NETK 2018. 24. o.

[43] Bővebben: https://coinmap.org

[44] KOVÁCS Zoltán: Az infokommunikációs rendszerek nemzetbiztonsági kihívásai, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, Phd értekezés 114.o.

5. Mekkora a veszélyeztetettség?

A kriptovaluták piaci értéke nagyon nagy volatilitást mutat. A közismert kriptovaluták esetében is sokszor volt 10%-ot meghaladó árfolyamváltozás egy napon belül is.

E cikk írásának időpontjában a bitcoin a legértékesebb kriptovaluta és bár volt már az árfolyama 20.000 USD környékén is – jelenleg 7.364 USD-on áll. Ez piaci kapitalizációban[45] azt jelenti, hogy valamivel több, mint 34.000 milliárd forintot érnek ezek a kriptovaluták.[46]

Ezek az összegek meglehetősen nagyok, de nagyon nagyszámú személy tulajdonában vannak – a tulajdonosi szerkezet heterogén.

Annyit lehet feltételezni, hogy a bitcoin rejtélyes és a mai napig ismeretlen feltalálója/fejlesztője Satoshi Nakamoto a mai napig tulajdonol hozzávetőleg 1 millió bitcoint[47]. Ezek a kriptovaluták a 2009. január 3-ai indulást követően kialakultak[48], de az óta változatlanul vannak ugyanazon tárcákban[49]. Ha valamilyen oknál fogva a feltaláló(k) értékesítenék ezeket a bitcoinokat, azt mindenki észrevehetné, hiszen a blokkláncból ez látható.

A bitcoin – mint a legjelentősebb kriptovaluta – becsült tranzakciós értéke naponta e cikk írása során – amikor az árfolyam a korábbi legmagasabb ár körülbelül harmada – is egy milliárd USD körül mozog. Jelen fejezet írása során a létrehozott bitcoin tárcák száma meghaladta a 25 milliót.[50]

A kriptovaluták a blokklánc technológiának csupán egyik megvalósulási formái. A blokklánc technológia azt teszi lehetővé, hogy egy központi szerver működése nélkül egy egyenrangú hálózatban információk láncolata alakuljon ki olyan módon, hogy a korábban közölt információk integritása vitathatatlan.

E mellett fontos tulajdonság, hogy a blokkláncba információt felfűző entitások egyenrangúak.

---

[45] Bővebben: https://blockchain.info/hu/charts/market-cap – Market Capitalization

[46] Viszonyítási alapként Magyarország költségvetésének 2018. évi bevételi főösszege 18.751 milliárd forint, és a forgalomban lévő forint bankjegyek értéke 2016. évi adatok szerint 3.365 milliárd forint. A Shell óriásvállalat 2017. évben (piaci kapitalizáció jelenértéken) 62.000 milliárd forintot ért, az Allianz 22.576 milliárd forintot.

[47] Egyes vélemények szerint 1.148.800 BTC áll a tulajdonában, amivel bőven a leggazdagabb emberek 10-as listájába is bekerült árfolyamtól függően (bővebben https://news.bitcoin.com/people-keep-sending-satoshi-nakamoto-bitcoin/)

[48] Klitzke, Evan: How Many Bitcoins Did Satoshi Nakamoto Mine? https://eklitzke.org/how-many-bitcoins-did-satoshi-nakamoto-mine [2018.05.27.]

[49] Wile, Rob: Bitcoin's Mysterious Creator Appears to be Sitting On a $5.8 Billion Fortune. http://time.com/money/5002378/bitcoin-creator-nakamoto-billionaire/ [2018.05.27.]

[50] https://blockchain.info/hu/charts/my-wallet-n-users [2018.06.02.]

A más területeken történő alkalmazhatóság folyamatosan foglalkoztatja fintech cégeket, pénzügyi vállalkozásokat, feltalálókat és állami szereplőket.

Vannak teljesen új megoldások, amelyek egyfajta új helyi pénzt hoznak létre a blokklánc technológia segítségével úgy, hogy az akár minden internettel kapcsolatban álló ügyfél számára elérhető.[51]

A blokklánc technológia számos fejlesztési lehetőséget nyitott meg. A nagy pénzügyi szolgáltatók is vizsgálják annak lehetőségét, hogy miként tudják rendszereik hatékonyságát növelni használatával.[52]

Amikor arra van szükség, hogy bizonyos információ megváltoztathatatlanul rendelkezésre álljon a felhasználók széles tábora számára és azt egy központi egység kompromittálásával ne lehessen befolyásolni, akkor megoldást jelenthet a blokklánc technológia.

Ukrajnában és Grúziában[53] a közigazgatási rendszer egyes elemeit – például a földhivatali nyilvántartást – a blokklánc technológiára alapítva fejlesztik.[54] Észtország forradalmian új tervekkel 2017-ben közzétette, hogy az Euro-hoz kötött nemzeti kriptovalutát kíván kibocsátani[55], de végül bejelentette, hogy nem valutaként kívánják bevezetni az EstCoin-t, hanem az e-állampolgárságot támogató informatikai rendszerként[56].

Ha elképzelünk egy olyan rendszert, amelyben minden személy, aki előzetesen azonosította magát (pl.: ügyfélkapun keresztül történő azonosítás) egy blokklánc technológián alapuló közzétételt tudna eszközölni arról, hogy eltulajdonították a gépjárművét. Egy egyenrangú hálózatban ez az információ gyorsan szétterjed minden címzettnek, így akár egy közlekedési csomópontban üzemelő rendszámfelismerő rendszernek, ahol aztán jelzés indulhat a rendészeti szerveknek a szükséges intézkedések megtételére.[57]

---

[51] Ilyen például a Mycelium Card, amely az összes szükséges hardver elemet is kifejlesztette a fizetési megoldásához – bővebben: https://card.mycelium.com/

[52] https://entethalliance.org/enterprise-ethereum-alliance-becomes-worlds-largest-open-source-blockchain-initiative/ [2018.06.10.] illetve https://bitport.hu/ma-mar-nem-az-it-cegek-mondjak-meg-mit-kell-vasarolnia-egy-banknak [2018.06.10.]

[53] Jellemzően az esetleges jogellenes, vagy korrupciós okból bekövetkező módosítások megelőzése érdekében.

[54] https://www.reuters.com/article/us-ukraine-bitfury-blockchain/ukraine-launches-big-blockchain-deal-with-tech-firm-bitfury-idUSKBN17F0N2?il=0 [2018.06.10.]

[55] https://www.ccn.com/estcoin-estonia-could-soon-launch-its-own-digital-currency/ [2018.06.10.]

[56] https://www.bloomberg.com/news/articles/2018-06-01/estonia-curbs-cryptocurrency-plan-that-drew-rebuke-from-draghi?srnd=cryptocurriences [2018.06.10.]

[57] Az ötlet logikusnak tűnik, de a megvalósítást illetően megoldható volna a hagyományos szerver-kliens kapcsolaton keresztül is, így előnye annyi maradna, hogy bármelyik csomópont kiesése esetén

Egy másik problémával kapcsolatban is működőképes megoldást jelenthetne a blokklánc technológia: a gépjárművek kilométer órájának visszatekerése szerte Európában komoly gondot okoz. Ha azonban kialakításra kerül egy rendszer, amelyben minden regisztráló gépjárműhöz egy kulcspárt kerül hozzárendelésre és számos autószerelő műhely, műszaki vizsgaállomás, vagy akár benzinkút megkapja a jogot, hogy a nyilvános kulcshoz tartozó blokkra információt fűzzön, akkor a tulajdonosnak a gépkorcsi értékesítésekor hiteles és megváltoztathatatlan blokklánc információ állna a rendelkezésére a privát kulcs felhasználásával, hogy milyen a jármű futásteljesítménye, milyen szerviz beavatkozásokat hajtottak rajta végre, de akár hogy mennyi volt jellemzően a fogyasztása.

Nem meghatározható, hogy a kriptovalutákkal összefüggő növekvő tendenciának mekkora hányada kapcsolódik Magyarországhoz, de a különféle szolgáltatások, internetes fórumok, médiamegjelenések azt mutatják, hogy hazánkban is egyre jelentősebb a kriptovaluták irányába megjelenő figyelem.

Fontos azonban azt is megjegyezni, hogy a Satoshi által lefektetett elvek szerint működő bitcoin sem egy végleges és változtathatatlan produktum. Ahogy az internet megalkotói sem gondoltak arra, hogy mekkora fejlődésen fog átesni a világháló,[58] úgy az eredeti tervek is megváltoztak. Ezt a változást egy nem teljesen egységes fejlesztői csoport valósítja meg.[59] Bár a forráskód nyilvános, de a további fejlesztések eredményezhetik a bitcoin rendszerének hibáit és akár hanyatlását is.

Összességében tehát látható, hogy:

– a kriptovaluták jelentős változást hoztak a pénzügyi kultúrában,
– a blokklánc technológia az élet számos területén ad forradalmian új megoldásokat.

Van, aki befektetési jelleggel, van, aki a technológiai újdonságok felé tanúsított érdeklődéssel, és van, aki a bűnös vagyonának elrejtésére, vagy más bűnös tevékenység céljaként, vagy eszközeként tekint a kriptovalutákra. Témánk szempontjából a bűncselekményekhez való kötődése érdemel kiemelést.

is tökéletesen működőképes maradna és az ügyfelek azonnal meg tudnák osztani az információkat.

[58] Az internet hajnalán még elképzelhetetlennek tartották, hogy az IPV4-es IP címek valaha elfogyhatnak, vagy hogy az internet ennyire átformálja a gazdaság és a modern társadalmak működését.

[59] The Bitcoin Foundation, Inc. nevű szervezet legfőbb célja Satoshi Nakamoto elveinek tovább folytatása, fejlesztése, népszerűsítése. https://bitcoinfoundation.org/website-terms-service/ [2018.06.08.]

6. Rendészeti kihívások, válaszok

A kriptovaluták piaci kapitalizációja tehát jelenleg nem jelentős. Ha a blokklánc technológiába vetett bizalom megrendül, akkor a XIX. századi aranyláz könnyen lecsenghet.

A bitcoin árfolyamának alakulásában az árfolyamcsökkenések mögött jellemzően a bizalomvesztés jelent meg:

- egyes bitcoin brókereket ért támadások, általuk elkövetett visszaélések,[60]
- állami szabályozók negatív hatása – jellemzően elfogadás tiltása – szintén hátrányos a kriptovaluta megítélésére,[61]
- más kriptovaluták irányába elmozduló érdeklődés,
- a kriptovalutát működtető informatikai háttérben való bizalomvesztés[62]

Nem kell konspirációs teóriákra gondolnunk, ha azt feltételezzük, hogy a pénzügyi szolgáltatók intézkedéseket tesznek, vagy akár lobbiznak annak érdekében, hogy a kriptovaluták elfogadhatósága csökkenjen. A pénzügyi eszközök bankrendszertől független tárolása, kezelése, transzferálása számukra bevétel kiesést eredményezhet. Jelentős érdekek léteznek az irányba, hogy a blokklánc technológia és a kriptovaluták a bankrendszeren belülre kerüljenek, vagy elfogadhatóságuk csökkenjen.

Állami oldalról egyrészt támogatandó minden innovatív technológia, amely a polgárok jóléte irányába hat[63], de csak addig a mértékig, amíg a hátrányok ezt meg nem haladják. Melyek lehetnek ezek:

- a bankrendszer bevételének csökkenése által az állami bevételek csökkenése,[64]
- a technológia használatában fejlettebb szinten álló külföldi szolgáltatóknál jelentkeznek inkább bevételként a kriptovalutákhoz kapcsolódó költések,[65]
- ha a technológia nem váltja be a hozzá fűzött reményeket, akkor az erre a célra elköltött javak nem térülnek meg, így összgazdasági hátrányt okoznak,

[60] Bővebben lásd: https://cointelegraph.com/tags/mt.gox

[61] Bővebben például: https://economictimes.indiatimes.com/wealth/personal-finance-news/your-bank-will-not-allow-you-to-buy-bitcoins-anymore/articleshow/63627123.cms

[62] Példaként említhető az ún. DAO csalás – bővebben: https://www.coindesk.com/understanding-dao-hack-journalists/

[63] Bizonyos feladatok költséghatékony, visszaélésektől mentes ellátása pl. a korábban említett célokra.

[64] Természetesen itt kérdésként merül fel, hogy az ügyféli oldalon jelentkező költségcsökkenésből származó megtakarításaikat mire fordítják az ügyfelek

[65] Itt a kedvező külkereskedelmi és fizetési mérlegre merkantilista szempontból tekintve mindenképpen előnyös a fejlettebb államok számára

– az állampolgárok kriptovalutákkal összefüggésben elveszítik anyagi javaik egy részét[66].

Ezen problémák elhárításában, megszüntetésében a rendészeti szerveknek érdemben nincs tennivalójuk, de melyek azok a hátrányos folyamatok, melyek feladatot adnak?:

– Az elmúlt években az Europol az internetes szervezett bűnözői fenyegetettségről szóló jelentéseiben is felhívta a rendvédelmi szervek fokozott figyelmét arra, hogy a kriptovaluták bűnelkövetési célú felhasználása egyre gyakoribb.[67]
– A kriptovalutákhoz köthető bűncselekmények sértettjévé válhatnak az állam polgárjai, illetve vállalkozások (csalások[68], információs rendszerek elleni támadások[69], tőkepiac-felügyeleti intézkedések hiánya). Ebben a körben bűnmegelőzési kampányok indítása volna célszerű a kriptovalutákhoz kapcsolódó piaci szereplők bevonásával olyan felületeken, amelyeket a lehetséges sértettek látogatnak – például kriptovalutákkal foglalkozó weboldalakon, fórumokon, szakmai rendezvényeken.
– A kriptovaluták anonimizáló, és földrajzi határokra érzéketlen tulajdonságainak kihasználása a bűnelkövetés során (pl. zsaroló vírusok[70], pénzmosás[71], terrorizmus finanszírozása).
– A bűnös forrásból származó vagyon elrejtése kriptovalutákban.

Ezen utóbbi problémák elleni fellépésben a bűnüldöző szervek további hatékony lépéseket kell tegyenek:

– Szükséges részt venni a jogalkotásban annak érdekében, hogy a kriptovalutákkal kapcsolatos szolgáltatások nyújtását magyar vállalkozások is jogszerűen és megfelelő ellenőrzés mellett végezhessék.[72]

---

[66] Itt nem jogsértő cselekményekre, hanem helytelen döntésekre, a piac várható mozgásának helytelen prognosztizálására kell gondolnunk

[67] Lásd Europol: Internet Organised Cybercrime Threat Assessment 2014-2018.

[68] Lásd Eszteri Dániel: Egy bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. Infokommunikáció és jog 2017/1. 25-31. o.

[69] Eszteri Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén és a tulajdon helyzetének magán- és büntetőjogi elemzése virtuális közösségekben. Doktori értekezés. Pécs, 2015. 204-207. o.

[70] Nagy Zoltán András – Mezei Kitti: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa In: Gaál Gyula – Hautzinger Zoltán (szerk.) Szent Lászlótól a modernkori magyar rendészettudományig. Pécsi Határőr Tudományos közlemények 19. Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2017. 165. o.

[71] Nagy Zoltán András – Mezei Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog 2018/1. 27-28. o.

[72] Ne legyen szükség más államokban (pl: Anglia) létesített vállalkozások fióktelepeként működtetni a vállalkozásokat.

– A létrejövő és a pénzügyi rendszerbe becsatlakozó fintech cégekkel partneri viszony kialakítása és közös elemző-értékelő rendszerek működtetése a pénzmosás gyanús tranzakciók kiszűréséhez.
– Az új büntetőeljásról szóló 2017. évi XC. törvény nevesíti az elektronikus adatot mint bizonyítási eszközt, valamint a rendelkezései alapján lehetővé válik az olyan virtuális vagyonelemek lefoglalása, mint a bitcoin vagy az elektronikus pénz speciális formái. Az új szabályozásnak köszönhetően a fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, hogy az elektronikus adattal olyan műveletet végeznek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét megakadályozza.[73] Azonban a büntetőeljárásokban[74] felmerülő kriptovaluták lefoglalása, kezelése érdekében szükséges egy módszertani utasítás kimunkálása az ügyészséggel közösen, az egységes joggyakorlat megteremtése érdekében.
– Szükséges a blokklánc technológiához kapcsolódó ismeretek elmélyítése a bűnüldöző és titkosszolgálati szervek állományában.[75]
– Fontos kiaknázni a bűnüldözési célú nemzetközi együttműködésből származó lehetőségeket: megismerni a legjobb gyakorlatokat, esettanulmányokat, részletszabályozási megoldásokat, használni a közös erőforrásokat.[76]

Stratégiai szinten az egyes államok számára fontos az összehangolt magatartás. Megítélésem szerint nem jelent megoldást a kriptovaluták túlzott tiltása, mivel azok a bűnelkövetéshez történő felhasználást csupán megnehezítik, de emellett nehezen felderíthetővé is teszik. Szükséges a törvényi szigorítás, de nem olyan mértékben, hogy az az innováció elfojtása mellett az elkövetők konspirációjához vezessen, ha-

[73] Be. 315. § (1) és (2) bekezdései; Lásd bővebben az elektronikus adat lefoglalásáról és megőrzéséről: Czine Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018.

[74] Lásd Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/1. 639-647. o.; valamint Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2. 125-126. o.

[75] Lásd ehhez Furneaux, Nick: Investigating cryptocurrencies – Understanding, extracting and analyzing blockchain evidence. Wiley, 2018.

[76] Lásd bővebben az európai és nemzetközi erőfeszítésekről a kibertér védelme érdekében: Parti Katalin – Kiss Tibor: Az informatikai bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): Kriminológia. Wolters Kluwer Kft., 2017. 510-514. o.; Szongoth Richárd – Vetter Dániel: Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. Belügyi Szemle 2018/7-8. 7-21. o.; Továbbá például az Európai Rendőrség (Europol) EC3 blokklánc elemző platformját vagy a United Nations Office on Drugs and Crime (UNODC) képzéseit: https://www.unodc.org/unodc/en/frontpage/2017/May/unodc-launches-training-to-tackle-money-laundering-and-bitcoin-banking-fraud.html

nem olyan mértékben, hogy abból a bűnüldöző és titkosszolgálati szervek információt szerezhessenek.

Mekkora erőforrást kell delegálni a rendészeti szervek részéről a kriptovalutákkal kapcsolatos problémák orvoslására? Sajnos azt nehéz meghatározni. Azonban az tény, hogy 2012. és 2017. között 141 ügy kapcsolódott a kriptovalutákhoz, ami összességében nem magas szám, de az emelkedés a 2012. évi 1 büntetőügyhöz képest a 2017. évi 58 ügy egy exponenciálisan emelkedő görbét mutat.[77]

Vélhetően a következő években sem valósulnak meg a kriptovalutákkal kapcsolatban olyan bűncselekmények, melyek Magyarország gazdasági érdekét érdemben befolyásolnák, hiszen nem nagy az ország kitettsége. Azonban az valószínűsíthető, hogy nagyszámú sértettet érintő jogsértések kerülhetnek napvilágra. Ezen túlmenően az is fontos szempont kell legyen, hogy az állampolgárok nyomozóhatóságokba vetett bizalmát és megbecsültségét nagyon pozitívan befolyásolná, ha az ilyen ügyeket szakértő módon, gyorsan és eredményesen fejeznék be a hatóságok.

Felhasznált Irodalom

Bakó Tamás: Bitcoin hálózatok elemzése (Diplomamunka). Eötvös Loránd Tudományegyetem, Természettudományi Kar, Matematikai Intézet 2015.

Czine Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018.

Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2.

Eszteri Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Doktori értekezés. Pécs, 2015.

Eszteri Dániel: Egy bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. Infokommunikáció és jog 2017/1.

Europol: Internet Organised Cybercrime Threat Assessment 2014-2018.

Franco, Pedro: Understanding Bitcoin: Cryptography, engineering and economics. Wiley, 2015.

Furneaux, Nick: Investigating cryptocurrencies – Understanding, extracting and

[77] Készenléti Rendőrség – Nemzeti Nyomozóiroda – Kiberbűnözés Elleni Főosztály témakutatásából.

analyzing blockchain evidence. Wiley, 2018.
Halász Viktor: Kriptovaluták a bűnüldözésben – új kihívások és lehetséges válaszok (Diplomamunka). NKE NETK 2018.
Kovács Zoltán: Az infokommunikációs rendszerek nemzetbiztonsági kihívásai, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, Phd értekezés
möser, Malte: Anonymity of Bitcoin Transactions. 2013.
Nagy Zoltán András – Mezei Kitti: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa In: Gaál Gyula – Hautzinger Zoltán (szerk.) Szent Lászlótól a modernkori magyar rendészettudományig. Pécsi Határőr Tudományos közlemények 19. Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2017.
Nagy Zoltán András – Mezei Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog 2018/1.
Parti Katalin – Kiss Tibor: Az informatikai bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): Kriminológia. Wolters Kluwer Kft., 2017.
Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/1.
Szongoth Richárd – Vetter Dániel: Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. Belügyi Szemle 2018/7-8.

SZATHMÁRY ZOLTÁN

AZ INTERNET MINT A BŰNCSELEKMÉNYEK ELKÖVETÉSÉNEK HELYE

1. Bevezető

Az információs társadalom egyik legszembetűnőbb jellemzője a mindent körülvevő infokommunikációs eszközök számának, sokféleségének és komplexitásának növekedése.[1] Az új technológia befogadásával kölcsönhatásban, így megismerésével, alkalmazásával, fogyasztói igények szerinti fejlesztésével a befogadó közeg, a társadalom is változik, a környezeti változások pedig egyúttal a jogalkalmazást is alkalmazkodásra kényszerítik.

A büntetőjogi diskurzusoknak kezdetektől részét képezi az internet közvetítésével elkövetett bűncselekmények miatt indult büntetőeljárásokban az illetékességet, illetve joghatóságot érintő kérdések rendezésére való törekvés. A későbbiekben részletesebben is vizsgált bírói gyakorlat alapján úgy tűnik, máig nem sikerült az internet helyét megtalálni és összeegyeztetni az illetékesség és joghatóság territoriális fogalmi alapokon nyugvó értelmezési közegében. Az illetékesség és joghatóság megállapítását megalapozó körülmények közül kiemelkedik a bűncselekmény elkövetésének helye, de ugyanezzel a földrajzi kérdéssel küszködnek a bűnüldöző hatóságok adatgyűjtő tevékenységének korlátaival foglalkozó szabályozási törekvések is.

E kérdések értelmezési kereteit az interneten zajló információáramlás és az alapvetően földrajzi alapú szabályozási tárgyra épülő dogmatikai rendszer jelöli ki. Az illetékesség kapcsán kialakult, és majd a későbbiek során ismertetett bírói gyakorlat értékeléséhez nem mellőzhető ennek a fejlődő technológiai közegnek a rövid bemutatása, amelynek révén felismerhetővé válik, hogy a joggyakorlat jelenlegi útkeresése a technikai fejlődésnek egy már meghaladott állapotára próbál reagálni. A technológiai elem jellemzője az említett társadalmi kölcsönhatásban a következő pontokban foglalható össze: az innovációk által életre hívott új technológiai rendszerek megjelenése között múló idő rövidül, az infokommunikációs eszközök tel-

[1] KINCSEI Attila: Technológia és társadalom az információ korában. In: BALOGH G. (szerk.) Az információs társadalom, Gondolat-Új Mandátum, Budapest 2007. 47. o.

jesítménye növekszik, valamint a számítástechnika, a telekommunikáció és a média konvergenciája figyelhető meg.[2]

2. Az információs társadalom technológiai szemlélete

2.1. Út a PC-től a digitális konvergenciáig

A folyamat kiinduló pontja a gazdaság, a tudomány és a társadalom egésze számára hozzáférhető, az adatok automatizált feldolgozását, továbbítását, tárolását lehetővé tevő számítógép megjelenése, amely lehetővé tette az emberi szellemi tevékenység kiváltását, illetve hatékonyabbá tételét, ezzel új, hozzáadott értékű szolgáltatások és javak teremtését biztosító kapacitáshoz juttatva a felhasználókat. Döntő szakasza volt a fejlődésnek, hogy a katonai és tudományos élet területéről kitörve az egyre kisebb méretű, egyre könnyebben kezelhető ám több perifériát csatlakoztatni képes és olcsóbb számítástechnika egyre több ember számára vált hozzáférhetővé.[3]

A következő szint a korábban elszigetelt, önálló egységek hálózatban történő összekapcsolása és az internet megjelenése volt. A világháló a kliens-szerver architektúrák világméretű kiépülése mellett a különféle P2P hálózati rendszerek, grid-rendszerek, és hyperszámítástechnikai rendszerek megjelenésével fejlődött tovább, az újabb fejlesztéseknek meghatározó technológiai alapjává, megannyi szolgáltatás önálló platformjává válva. Közben a személyi számítógépek mellett az emberi környezet egyre több elemében jelentek meg infokommunikációs eszközök (pl: gépkocsik fedélzeti számítógépe, háztartási berendezések, ún. intelligens otthonok rendszerei), amely egy korszak, a desktop-számítógépek dominanciájának lezárulását eredményezte.

A technológia fejlődésének irányát a miniatürizáció, mobilizáció, a funkciók konvergenciája, a hálózati működés, valamint mindezek szabványosítása határozzák meg, amelyek hatására újabb és újabb infokommunikációs eszközök váltak minden ember számára elérhetővé (pl.: laptop, okostelefonok, tabletek, stb.).

A komplex személyi hírközlési eszközök integrálták a mobil távközlés, a kép- és mozgóképrögzítés, a hang- és videoalapú szórakoztatás, a navigáció funkcióit, a különböző szolgáltatásokhoz tartozó személyazonosító kártyákat, az elektronikus aláírást, és fizetési módokat.

[2] Kincsei: i.m. 59-60. o.

[3] Az IBM 1981-ben dobta piacra a már nevében is személyeknek szánt PC-t, azaz a personal computer-t.

A folyamat egyik kulcsfogalma tehát a konvergencia, amelynek bár nincs pontos, általánosan elfogadott használata a szakirodalomban, a téma szempontjából különböző hálózati platformok azon képességét jelenti, hogy alapvetően hasonló szolgáltatási fajtákat hordoznak, de olyan fogyasztói eszközök összefonódását is jelöli, mint például a telefon, televízió és a személyi számítógép. Meghatározó technológiai alapja a digitalizáció, amely műszaki megoldás lehetővé teszi, hogy ugyanaz a tartalom a korábban egymástól elkülönült hálózatokon is átvihető legyen.[4] Koppányi Szabolcs szerint[5] a tapasztalható változás úgy jellemezhető, hogy az információk megjelenési formája kompatibilissé vált, ennek következtében az információhoz különböző kommunikációs eszközök közvetítésével (internet, telefon, televízió) hozzájutva elmosódnak a határok mind a tömeg- és az egyéni kommunikáció, mind pedig az elosztó és közvetítő médiumok között.

A digitalizáció a tartalmak platformfüggetlen közvetítésének fejlődésével a korábban elkülönült gazdasági ágazatok, úgymint az informatika, a távközlés és a média közeledését, összeolvadását is elindította. Maga a konvergencia tehát nem egységes jelenség, a szűkebben vett technikai fejlődés, a gazdasági struktúrák változása, valamint a fogyasztói viselkedések konvergenciája egy időben zajlik. E folyamat figyelemmel kísérésére többek között azért van szükség, mert meghatározza az informatikai bűncselekmények elkövetésének környezetét infrastrukturális, gazdasági és társadalmi értelemben is.

2.2. A technológiai fejlődés társadalmi aspektusai

A közelmúlt és a jelen technológiai szemléletű információs társadalmát tovább jellemezhetjük három társadalmi terület konkrét változásai alapján is.[6] Az üzleti szféra tekintetében az elektronikus kereskedelemben az infokommunikációs eszközök és szolgáltatások terjedésével a vevőkapcsolatok új formái jelentek meg. Egy vagy több termékcsoportra szakosodott elektronikus piacterek születtek, amelyek sok termék tekintetében rövid időn belül háttérbe szorították a hagyományos vásárlási fórumokat.

Az új, fizetési eszközök (fintech megoldások) a készpénzforgalmat, a mesterséges intelligencia[7] és a robotika a tőzsdei kereskedések emberi döntéseit helyettesítik, egyre kényelmesebbé, hatékonyabbá téve eddigi tevékenységeinket. Az infokom-

[4] Tóth András: Az elektronikus hírközlés és média gazdasági szabályozásának alapjai és versenyjogi vonatkozásai, HVG-ORAC Budapest, 2008. 57. o.

[5] Koppányi Szabolcs: Hírközlési jog az európai közösségben és Magyarországon, Osiris Kiadó Budapest, 2003. 23. o.

[6] Dömölki Bálint (szerk.): Égen-földön informatika. Typotex, Budapest, 2008. 25-44. o.

[7] Lásd Eszteri Dániel: A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései. Infokommunikáció és jog. 2015/2-3. 47-57. o.

munikációs eszközök megreformálták az elektronikus üzletvitelt az üzleti folyamatok automatizálásával, a közvetlen termelésirányítás és logisztika informatizálásával lehetőség nyílt a piackutatás, a költséghatékonyság, a termelékenység további javítására. Mindezek mellett természetesen új üzletágak is megjelentek, például: a tartalomszolgáltatás, pénzügyi és bankinformatika, tudásmenedzsment, kutatásfejlesztés, stb.

A közszféra változásai például a közigazgatás informatizálásában nyilvánulnak meg. A kormányzati portál, az elektronikus ügyfélkapu, a regisztrált tulajdonok (gépjármű, ingatlan) és cégjegyzék elektronikus nyilvántartása, az igazságügyi intézmények elektronikus ügyvitele[8], valamint a társadalombiztosítási és egészségügyi szervezetrendszer mind-mind infokommunikációs hálózatok üzemeltetésével törekednek az állam működésének, az állam és polgára közötti kapcsolat javítására.

Végül a magánfelhasználás területén nemcsak a személyek közötti kapcsolattartás alakult át, hanem az otthoni életvitel és háztartási információkezelés is, a szabadidő eltöltésének lehetőségei, az alkotóművészet, munkavégzés és még számos egyéb aktivitás. A magáncélú kommunikáció új trendjei megszüntették a média egyirányúságát, helyét átvette az interaktivitás, azaz mindenki, minden felhasználó médium lehet. E korszakban már nem a PC, hanem a web működik platformként, ahol a felhasználók gyakran együttesen állítják elő, osztják meg egymással a tartalmakat interaktív alkalmazások segítségével.

A technológiai elem (az eszközök és szolgáltatások) biztosítja a társadalom számára az intenzívebb információáramlást, az információk tömegéhez való hozzáférést, míg a társadalom oldaláról nézve a hagyományos, fizikai világbeli tevékenységek infokommunikációs technológiai rendszerekkel történő támogatottsága, mediatizáltsága magának a tevékenységnek a virtuális dimenziójába való kiterjesztését eredményezi.[9] Ezen eszközök relatíve általánosan hozzáférhető volta lehetővé teszi a társadalom minden tagja számára a nemzethatárokon átívelő kommunikációt, kapcsolatteremtést, közösségépítést, megváltoztatva ezáltal a felhasználók szokásait, a magánélet színtereit.

2.3. A KOMMUNIKÁCIÓ ÉS KÖRNYEZETE

A kommunikáció nem csak személyek között zajlik, hanem egyre inkább a technikai környezet és az ember között is. Az ember-gép interakcióját tekintve az egyre

[8] Pl.: az ingatlan-nyilvántartás elektronikus alapú TAKARNET-rendszere, a bűnügyi igazgatásban a Robotzsaru, Netzsaru, PraetorPraxis, a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala által üzemeltetett bűnügyi nyilvántartás, MAKÖR, stb.

[9] KINCSEI: i.m. 59-60. o.

több intelligens vonást mutató, számítástechnikai eszközök által behálózott környezetben a felhasználó személyre szabott módon tudja folytatni kommunikációját, biztosítva a fizikai lét mellett az állandó „online" jelenlétet. E területen folyamatosan zajlik a környezettel történő interakciók lebonyolítására szolgáló szenzorok (érzékelők) és aktuátorok (beavatkozók) fejlesztése, amelyek az emberi gesztusok, hangok érzékelése alapján hajtják végre az adott számítástechnika rendszer funkcióját. A szenzorok és aktuátorok a (nemcsak) virtuális környezetek és távközlési végberendezések kombinálódásával, ad hoc és vezeték nélküli rendszerré alakulásával a felhasználó cselekedeteit és interakcióit támogató környezet-intelligenciává alakult gépekként egyre inkább a hétköznapi élet szerves részévé válnak.

A vezeték nélküli, önkonfiguráló hálózatokká alakuló, tároló és feldolgozó kapacitással rendelkező apró eszközök, amikben a számítógép beágyazott célhardver formájában van jelen, fizikai tereinket benépesítve egyre fontosabb szerepet kapnak. Az embert, a felhasználót e tárgyakba épített intelligens interface-ek veszik körül, a személyre szabott technikai környezet szinte észrevétlenül felismeri jelenlétünket és reagál rá. Ez az intelligens felhasználói felület lehetővé teszi a környezettel való természetes, például hang vagy gesztusok általi, referenciáinknak és a kontextusnak megfelelő interakciót (például: közlekedési, helymeghatározási rendszerekre, helyváltoztatással kapcsolatos egyedi alkalmazásokra, vagy testbe épített implantátumokra lehet gondolni).[10]

Az „ember-gép" kommunikáció mellett természetesen a szintén egyre több intelligens vonást mutató M2M (machine to machine), „gép-gép" kapcsolatok, a robotika, mesterséges intelligencia területei is rohamosan fejlődnek, ám ezen trendek részletezése a tanulmány kereteit már meghaladnák.

2.4. Negyedik szint: a virtuális jövő

Az interakciók okán megnövekvő terhelés miatt a hálózati rendszerek hatékonyságának növelésére, az egyes rendszerelemek közötti koordináció és szinkronizáció lebonyolítására az ún. köztes szoftverek fejlesztése jelenti az egyik üzleti irányzatot. Felhasználói oldalon a növekvő alkalmazások és szolgáltatások okozta terhelés miatt az infrastruktúra hatékonyságának javítása érdekében alapvető érdek, hogy az informatika számára a prioritásokat ne a mindenkori technológiai adottságok átláthatatlan fejlesztése, hanem egyre inkább az üzleti igények és az igényelt szolgáltatás minősége határozza meg.[11]

[10] Dömölki: i.m. 2008. 61. o.
[11] Dömölki: i.m. 2008. 358-359. o.

Ezért a fejlődés újabb szintje az adat- vagy informatikai központok virtualizálódása, azaz olyan központok létrehozása (pl. az ún. felhő-szolgáltatások), ahol az egyes rendszerelemek helye, belső vagy külső volta, konkrét típusa egyre kevésbé játszik szerepet, míg az erőforrások igénybevétele a terheléstől függően dinamikusan változik.[12] A virtualizáció eredményeképpen a rendszer kifelé mutatott viselkedése, külső kapcsolatai és funkciói függetlenné válnak a rendszer belső architektúrájának fizikai felépítésétől, az informatikai erőforrások, a rendszerelemek absztrakt kezelésére lehetőséget nyújtva, azaz a technológia a fizikailag egyébként létező elemeket és működésüket más módon, más platformon logikailag jeleníti meg.[13]

Az informatikai rendszerek üzemeltetése egyre inkább közműjelleggel és szolgáltatásszerűen történik, ami részben abban nyilvánul meg, hogy a felhasználók személyi számítógépein futó programok mind nagyobb része kerül központi szolgáltatásként végrehajtásra, gyakran a felhasználó adatainak nagy részét is a szolgáltató szerverein tárolva. Ennek része, hogy a felhasználók adatai a szolgáltatók birtokába kerülnek, és azokra a felhasználónak pusztán csak igénye van. Az információtechnológiai közművek kialakulása felé mutató fejlődési irány a cloud computing. Ez esetben a szolgáltatók igen nagy számú felhasználót vagy különösen nagy leterhelést kezelni is képes szolgáltatásként nyújtják az információtechnológia által támogatott képességeiket. E jelenség mögött három irányvonal egymáshoz közeledése áll: a szolgáltatásorientáltság, a virtualizáció és az interneten keresztül bonyolódó számítástechnika szabványosítása.[14]

2.5. A jövőkép

A szüntelen technológiai fejlődés vizsgálatára irányuló kutatások alapján körvonalazható jövőkép elemei a következők. A számítógépek és adatátviteli vonalak teljesítményei oly mértékben növekednek, hogy gyakorlatilag nem jelentenek majd korlátot a megoldandó feladatok méreteire vonatkozóan. Teljessé válik az eszközök összekapcsoltsága, nem lesznek elszigetelten működő számítógépek. Az információfeldolgozás és adatátvitel lehetőségei megjelennek az embert körülvevő környezet tárgyaiban (pl. háztartási berendezések, járművek), akár az emberi testben (különféle bionikus protézisek, képességjavító implantátumok). Az informatikai rendszerek működése egyre több intelligens vonást mutat.

A rendszerekben a szolgáltatások különböző fajtái kerülnek előtérbe, a felhasználók mind inkább szolgáltatásokat és nem termékeket vásárolnak. Az infokommunikációs rendszerek fokozott mértékben támogatják az őket használó emberek

[12] Dömölki: i.m. 2008. 358-359. o.
[13] Dömölki: i.m. 2008. 66. o.
[14] Dömölki: i.m. 380. o.

együttműködésének különböző formáit. A fejlődési folyamat eredményeképpen az internet egyre inkább interface-szerepet tölt majd be a helyüket változtató emberek és az őket körülvevő fizikai világ között, végül olyan egységes és programozható rendszerré válhat, amely megtestesíti a korábbi kibertér[15] (cyberspace) víziókat.[16]

3. A technológiai környezet büntetőjogi szabályozási kérdései

Mi ennek a folyamatnak a témánk szempontjából kiemelhető jellemzője? A fentiekben röviden ismertetett, a közműszerű működés felé fejlődő információs hálózat funkciója továbbra is az információ feldolgozása, továbbítása, és az információhoz való hozzáférés biztosítása. Az internethálózat mint technika egyrészt tartalomsemleges, másrészt globális, ebből következik, hogy az adatok helye, az információfeldolgozás infrastruktúrájának egyes rendszerelemei – meghatározónak tűnő újszerűségük ellenére – nem kaphatnak minden esetben kiemelt jelentőséget az illetékességi és joghatósági kérdések rendezése során. Csak az internet igénybevételének egyes mozzanataira irányuló nemzeti szabályozás lehet kompatibilis az eddigi földrajzi alapú, állami fennhatóságot feltételező normarendszerrel. Az információs rendszerként értelmezhető internet – vagy egyes rendszerelemeinek – helye a legtöbb esetben egyébként sem értelmezhető.

Az infrastruktúra fenntartása és működtetése ugyan több szinten megosztott, de a rendszer meghatározó résztvevői olyan gazdasági szereplők, amelyek honossága ugyan kötődhet egyes államokhoz, azonban tevékenységüket globálisan végzik (pl. keresőszolgáltatások, DNS szolgáltatás, felhőszolgáltatások, stb). Azaz szemben egy-egy állami közműszolgáltatással, e szolgáltatások nyújtói egyre kevésbé tartoznak egy meghatározható állam vagy államok fennhatósága alá, de szolgáltatásaikat az állam(ok) polgárai számára minimum regionális, vagy kontinentális szinten nyújtják.

A szabályozás szempontjából lényeges elem ebben a rendszerben az is, hogy immár jellemzően nem a különféle érdekeket megtestesíteni képes elektronikus adatok birtoklása képvisel értéket, hanem az azokhoz való hozzáféréshez, a rendszer használatához, a rendelkezés lehetőségéhez kapcsolódik jogos érdek. Az állami fennhatóság, szuverenitás szempontjából így annak lehet jelentősége, hogy

[15] A kibertér fogalma William Gibson írótól származik, aki a Neuromancer című regényében a hálózatba kapcsolt számítógép-terminálokról közvetlenül elérhető digitális, navigálható teret jelöli vele. Gibson, W., Neuromancer. Harper Collins, London. 1984.

[16] Dömölki: i.m. 204. o.

a) az állam területéről igényelnek-e hozzáférést az adathoz, illetve az állam területén tesznek-e rendelkezést az adattal vagy az információs rendszerrel,
b) az állam területére irányul-e az adatok továbbítása, vagy az információs rendszer által végrehajtott művelet az állam területén fejti-e ki hatását,
c) az állam polgárának, honos jogi személyének vagy magának az államnak valamely jogszerű (személyi, vagyoni, gazdasági, biztonsági) érdeke érintett-e,
d) az állam polgárának, honos jogi személyének vagy magának az államnak valamely jogszerű (személyi, vagyoni, gazdasági, biztonsági) érdekét „megtestesítő" adatokat kezelő információs rendszer érintett-e.

Utóbbi két szempont a személyi elvet jeleníti meg, a területi elv alapjául szolgáló körülményként az első két pont értékelhető.

Ennek a globális közműnek az igénybevétele jellemzően a bűncselekmények elkövetésének eszközeként funkcionál, nincs jelentősége annak, hogy az adatok, a globális infrastruktúra egyes elemei hol találhatók, és hangsúlyozandó, hogy az információ-feldolgozás technikai folyamatában ez egyre kevésbe meghatározható. Leegyszerűsítve tehát e problémát, azon cselekvőségeknek, mozzanatoknak van jelentősége, hogy az információs szolgáltatást hol vették igénybe, az adatokhoz hol fértek hozzá, vagy hová irányították. Amennyiben valamely információs rendszer megbízható működéséhez fűződő érdeket sért a cselekmény, akkor kaphat jelentőséget ezen rendszer helye, vagy a felette rendelkező személye is. Ezek után vizsgáljuk meg a tipikus „internetes" bűncselekmények elkövetésének helyét illetően kialakult hazai joggyakorlatot.

4. Az illetékességet megalapozó körülmények

A magyar büntető joghatóságot elsődlegesen megalapozó körülmény az, ha a bűncselekményt belföldön követték el.[17] Az illetékességet illetően a büntetőeljárásról szóló 1998. évi XIX. törvény[18] 17. §-ának (1) bekezdése alapján – ha a törvény eltérően nem rendelkezik – az eljárásra az a bíróság illetékes, amelynek a területén a bűncselekményt elkövették. Ehhez képest kiegészítő rendelkezést rögzít a 17. § (3) bekezdése, amely alapján az eljárásra az a bíróság is illetékes, amelynek területén a terhelt lakik, ha az ügyész, a magánvádló vagy – ha e törvény másként nem rendelkezik – a pótmagánvádló ott emel vádat. Az új büntetőeljárásról szóló 2017.

[17] Btk. 3. § (1) bekezdés a) pontja
[18] A kézirat lezárásakor hatályban lévő jogszabály.

évi XC. törvény további lépéseket tett az elkövetés helyével kapcsolatos gyakorlati problémák eljárásjogi megoldása felé. Az új eljárási kódex alapján az ügyészség vádat emelhet immár a sértett lakó- illetve tartózkodási helyén is.[19] Úgy vélem az új szabály miatt nem szükséges az elkövetési hely körébe vonni az elkövetésnek a sértett tartózkodási helyével kapcsolatos mozzanatait.

Az illetékességet és joghatóságot megalapozó egyik alapvető körülmény tehát a bűncselekmény elkövetésének a helye. A bírói gyakorlat az elkövetés helyeként azonban nem a szoros értelemben vett elkövetési magatartás kifejtésének helyét tekinti. Ennek megfelelően a magyar joghatóság kérdését illetően a bűncselekmény belföldön elkövetettnek tekintendő, ha annak a magyar büntetőtörvény szempontjából jelentős bármelyik mozzanata – akár az elkövetési magatartás, akár az eredmény – belföldön valósul meg [BJD 4622.]. A joggyakorlat ellentmondásainak okai éppen a releváns elkövetési mozzanatok kiválasztására, az elkövetési mozzanatok mibenlétének eltérő felfogására, és az elkövetési magatartás kiterjesztő értelmezésének gyakorlati igényére vezethető vissza.

4.1. Tartalom-bűncselekmények

Tartalom-bűncselekményekként jelölöm azokat a bűncselekményeket, amelyek esetében az interneten hozzáférhető elektronikus adatok tartalma képezi a szabályozás tárgyát, ideértve a büntetőjogi tilalmat is. E csoportba sorolhatók pl. a szerzői és szomszédos jogot sértő bűncselekmények, a gyermekpornográfia, vagy a különféle titkot megtestesítő adatokkal való visszaélések. E bűncselekmények elkövetési magatartása alapvetően ezen tartalmakhoz való hozzáférésben, azok birtoklásában, illetve az adatokkal való különböző műveletek végzésében nyilvánul meg. Ezen bűncselekménytípusok estén az egyes adatok – kezelésének, birtoklásának – helye és az adatokkal való rendelkezés helye alapozza meg az elkövetés helyét. Az adatokkal való rendelkezés alatt az elektronikus adattal végzendő műveletre adott utasítást értem.

4.2. Közléssel elkövetett bűncselekmények

Következetesnek tekinthető az ítélkezési gyakorlat az olyan, közléssel elkövetett bűncselekményeket illetően is, mint az önbíráskodás, a csalás, vagy a zaklatás.[20] Ezen, információközléssel megvalósuló bűncselekmények sajátossága a célzatosság. A Btk. 222. §-a (2) bekezdésének a) pontja szerinti zaklatás vétségének tényállási eleme a félelemkeltési célzat, az önbíráskodásé és a csalásé pedig az, hogy a passzív

[19] 2017. évi XC. törvény 21. § (3) bekezdés
[20] BH 2013.87., BH 2011.332.; EBH 2000.292.

alany[21] a fenyegetés, illetve a megtévesztés hatására az elkövető akaratának megfelelően cselekedjen.

Ezért – ha e bűncselekmények közléssel valósulnak meg – azok szükségszerű feltétele, hogy az elkövetési magatartást megvalósító közlések a passzív alanyhoz eljussanak, a bírói gyakorlat szerint tényállásszerű elkövetési magatartásról csak ettől kezdve lehet szó. Erre figyelemmel a bírói gyakorlat szerint az elkövetés helye ilyen esetekben a közlésről való sértetti tudomásszerzés helye. A telefonon vagy levélben történt elkövetés esetén az elkövetés helye a hívás fogadásának, illetve a küldemény átvételének helye, interneten történő elkövetés esetén a megtévesztő közlést tartalmazó internetes honlap megnyitásának a helye.[22]

Utóbbi példa esetén úgy tekinthetjük e helyzetet, hogy az információ közlése a sértett tartózkodási helyén realizálódik, a közlés végpontjának ő tekinthető. Látható, hogy ezen esetekben a gyakorlat a kommunikációs kapcsolat két pontjából a végpontnak tulajdonít jelentőséget, a kommunikációs csatorna, a médium mibenléte lényegtelen. Ilyen esetekben tehát a megtévesztés akkor történik, amikor a konkrét sértett az interneten szembesült a vádlott megtévesztő szándékkal internetre feltett és azáltal közvetített csalárd közlésével.

Előfordulhat, hogy csalás esetében az elkövetési magatartás, a károkozó magatartás kifejtésének és a kár bekövetkeztének helye eltérő. A károkozó magatartás kifejtése és az eredmény bekövetkezte sem feltétlenül és értelemszerűen a sértett tartózkodási helyén történik, legfeljebb akkor, ha maga a sértett a tartózkodási helyéről kezdeményezi pl. a banki átutalást. Több sértett esetén a gondolamenet következetes érvényesítése furcsa helyzethez vezet. Ha az elkövető nem egy meghatározott személyt, hanem egy ismeretlen személyi kört (pl. termékhirdetéssel) akar tévedésbe ejteni, az elkövetés helye több helyszínt jelent, noha az elkövető az információkat egy helyről indította. A homogén alaki halmazat ezért nem teljesen illeszkedik az elkövetés helyét lehetőség szerint egy konkrét helyhez kötni igyekvő gyakorlati igényekhez.

Felmerül a kérdés, hogy miért szükséges az elkövetés helyeként kizárólagosan, illetőleg elsődlegesen a sértett tartózkodási helyét megjelölni. Az elkövetés helyének anyagi jogi meghatározása nem kívánt gyakorlati következményekkel – illetékességi problémákkal – jár, ezért azt eljárásjogi rendelkezések teszik kezelhetővé azzal, hogy az elkövetés helyéhez objektív körülményt társítanak. A terhelt lakóhelyén való vádemelés is ilyen másodlagos illetékességi ok.

[21] A vizsgált eseti döntések gyakorta a sértett kifejezést használják – jobbára a vizsgált eljárásjogi kérdések miatt –, de természetesen anyagi jogi kérdések esetén a passzív alany kifejezés használata a helyénvaló.
[22] BH 2011.332.

A BH 2011.332. számú eseti döntésben utalt arra a Legfelsőbb Bíróság arra is, hogy közömbös az internetes szolgáltató székhelye, valamint az adott ügyben a vádlott lakó-, illetve tartózkodási helye és bankszámlájának helye. Az első és utolsó kérdésben maradéktalanul osztani lehet az eseti döntésben kifejtett álláspontot. Ugyanakkor a megtévesztést megvalósító elkövetési magatartást illetően célszerű további finomításokat tenni. Előfordul, hogy az elkövető által megkezdett vagy kifejtett magatartásnak nincs egy meghatározott, célzott sértettje, az elkövető szándéka nem egy adott személy ellen irányult. Ezért a megtévesztő információk közlése valóban akkor „hatályosult", amikor a hirdetést valaki megtekintette. Ugyanakkor e kérdéstől teljességgel függetleníthető, és tényszerű, hogy az elkövető az internetet az információk közlésének eszközeként hol használta. Az elkövetési magatartás ugyanis csakis az elkövető által kifejtett és a külvilágban megjelenő esemény lehet, nem pedig az információs rendszer által megjelenített esemény.[23] Az elkövető a külvilágban a tartózkodási helyén tanúsított releváns magatartást, amelynek további eseményvonalai a kibertérben és a sértett tartózkodási helyén vetültek ki. Az elkövetés mozzanatai közül a sértett tartózkodási helyének kiemelése mellett nem szól meggyőzőbb érv, mint a terhelt tartózkodási helye mellett, hiszen az ismertetett infokommunikációs környezetben a kommunikáció egyik végpontja sem feltétlenül fix (pl. a sértett a vonaton ülve, telefonkészülékén olvassa a megtévesztő közlést).

Ahogyan arra a BH 2009.317. számú eseti döntés is kitér, az illetékességet az elkövetés más mozzanatai is megalapozhatják, így a csalás elkövetése esetén az elkövetési magatartás, a tévedésbe ejtés kifejtésének és az eredmény bekövetkezésének helye mellett a károkozó magatartás kifejtésének a helye is megalapozhatja a bíróság illetékességét.

Más esetben, amikor az internet nem kap szerepet a megtévesztő információk közvetítésében, a jogalkalmazás nem bonyolítja túl az elkövetés helyének értelmezését. Az ún. banki csalások esetén, az elkövető megtévesztő cselekménye és a sértett téves tudattartama kialakulásának helye gyakran eltér egymástól, hiszen más helyen történik a valós ügyleti szándék nélküli hiteligénylés és máshol annak elbírálása. Ez jellemzően intézmények „tévedésbe ejtésének" esetében fordul elő, amikor a tévedésbe ejtett passzív alany (banki alkalmazott) és a sértett személye (pénzintézet) személye elválik egymástól. Így, ha a pénzintézeti fiókban csalárd szándékkal szerződés megkötését kezdeményezik és a szükséges dokumentumokat benyújtják, míg a hitelbírálat attól elkülönült helyen történik, a csalás elkövetésének helyét a hiteligénylés helye megalapozza. Az elkövető által kifejtett cselekmény, a valótlan információk közlése már a bankfiókban megtörténik.

[23] Ez majd a mesterséges intelligencia által megvalósított események jogi értékelésének kihívásai között értékelhető.

Így az információt közvetítő közeg jellegének eltérősége nem igényli eltérő illetékességet megalapozó körülmény kizárólagos megállapítását. Azaz nem lehet kizárni az illetékességet megalapozó körülmények közül az elkövető tartózkodási helyét sem.

Az eseti döntések alapján megállapítható, hogy a csalás esetén az elkövetés helyének megállapítása szempontjából a bírói gyakorlat nem tulajdonít jelentőséget a megtévesztő információt, közlést tartalmazó adatok és információs rendszer helyének. Ennek hangsúlyozására azért volt szükség, mivel a rágalmazás és becsületsértés esetén ettől eltérő a gyakorlat.

4.3. Rágalmazás, becsületsértés az interneten

A viszonylag friss, a BH 2016.167. számú eseti döntésben megjelenő bírói gyakorlat szerint az interneten közléssel megvalósult rágalmazás, illetve becsületsértés esetén a bűncselekmény elkövetésének helye fő szabály szerint, elsődlegesen a kérdéses tartalmat közlő weboldalt működtető szerver helye. Az eseti döntés kiegészítő jelleggel, másodlagos szabályként úgy rendelkezik, hogy ha a weboldal külföldi székhelyű szerverről működik, a bíróság illetékességét a terhelt lakó-, illetve tartózkodási helye határozza meg.

Felmerül a kérdés, hogy mi az alapja ezen kettős, elsődleges és másodlagos szabály felállításának. Az eseti döntés alapján ugyanis az elkövetés helyét olyan semleges, technikai körülmény alapozza meg, mint az információközlésre szolgáló adat, illetve információs rendszer egyik elemének a helye. Úgy vélem, a már korábban elemzett technológiai környezetben az említett körülmény kiemelése indokolatlan.

Az infokommunikációs közeg jellemzőire az eseti döntés maga is hivatkozik, érvelése szerint „a technika fejlődésével ma már széles körben elérhetővé váltak és elterjedtek azok a mobil technikai eszközök (például laptop, tablet, az ún. „okostelefon"), melyek az internet elérésére és az azon való kommunikációra szinte bárhonnan, egyszerűen alkalmazhatók, méretüknél fogva pedig könnyedén hordozhatók is. A mobilinternet-szolgáltatások szinte az egész országot lefedik, és számos helyen gyors, vezeték nélküli internetcsatlakozás is nyilvánosan, bárki részére rendelkezésre áll. Lényegében tehát bárhonnan – közterületről, más épületből vagy akár utazás közben is – hasonló egyszerűséggel és alacsony költségráfordítással érhető el az internet, amint otthoni körülmények között is. Így tehát egyáltalán nem biztos, sőt még csak nem is valószínűsíthető, hogy az internetre közlést eljuttató személy azt a lakóhelyéről teszi meg. Következésképp „az elkövető lakóhelye a rágalmazó vagy becsületsértő kijelentés ott történt leírására vonatkozó konkrét adat hiányában nem lehet a Be. 17. § (1) bekezdése szerinti illetékességi ok alapja."

Az eseti döntés érvelésével eddig a pontig maradéktalanul egyet lehet érteni. Azonban úgy folytatódik, hogy „[h]elytelen az az álláspont, amely az elkövetés helyének azt a helyet tekinti, ahol – feltételezésük szerint – az elkövető a számítógépén

a feljelentésben sérelmezett kijelentéseit megszerkesztette, és ahonnan azt az üzemeltető szerverére küldte." Álláspontom szerint ez a következtetés nem következik szükségszerűen az azt megelőző érvekből, emellett a döntés indokolása utal az elkövető cselekményeire vonatkozó adatok hiányára is, ezzel pedig úgy tűnik, nem zárja ki egyértelműen az elkövetés helyeként az elkövető tartózkodási helyét.

Az elkövető lakóhelye valóban nem meghatározó az internetszolgáltatás igénybevételét illetően, de ettől még a tartózkodási helyet nem lehet kizárni az illetékességet megalapozó körülmények közül, és az adat helyét megtenni illetékességet megalapozó körülményként. Hiszen ahogyan azt az eseti döntés indokolása is kifejti, az elkövetés helye valójában a tényállásszerű magatartás kifejtésének, illetve kifejtése megkezdésének a helye.

A csaláshoz hasonlóan közléssel megvalósuló bűncselekmények esetén az elkövetés helyének a csalástól eltérő elvi alapon nyugvó megállapítását az eseti döntés a következőképpen indokolja. A Btk. 226. § (1) bekezdése értelmében a rágalmazást „más előtt", a Btk. 227. § (1) bekezdése szerint a becsületsértést pedig „mással szemben" kell megvalósítani. Az eseti döntés indokolása szerint ez a becsületcsorbító tényállításnak vagy kifejezésnek a számítógépen való megszövegezésével – anélkül, hogy arról bárki tudomást szerzett volna – objektíve nem valósul meg. Az eljárás tárgyát képező kijelentések „írásba foglalásának" helye tehát nem lehet az elkövetés helyének tekinthető. Erre nézve az eseti döntés a már ismertetett, ugyancsak közléssel elkövetett bűncselekmények (önbíráskodás, csalás, zaklatás) esetében kialakult ítélkezési gyakorlatra utal vissza (BH 2013.87., BH 2011.332.; EBH 2000.292.).

Ezen a ponton azonban az eseti döntés eltérő szempontokat vesz figyelembe, és csak részben az analóg információközlés elveire alapítja érvelését a digitális információközlés környezetével szemben. Ezért vitatható az eseti döntésnek ez a megállapítása. Az elkövetési magatartás kimerülhet abban, hogy az elkövető megfogalmazza a becsületsértő szöveget, ha az egyúttal automatikusan hozzáférhetővé válik a nyilvánosság számára. Az online közösségi média eltér azon médiától, amely a sajtó útján elkövetett rágalmazásokra vonatkozó joggyakorlatot kialakításának igényét felvetette, a felhasználó maga válik tartalomszolgáltató médiummá. Az elkövető magatartása az internetszolgáltatás igénybevételének utolsó mozzanatáig tart, az pedig a szöveg elhelyezésére irányuló rendelkezése, pl. a közösségi oldal szolgáltatásának (kommentelés) igénybevétele, pontosabban az igénybevételt megvalósító rendelkezése.

A rágalmazás tényállásának alapvető eleme azon hely, ahol a tény állítására, híresztelésére, illetve a tényre közvetlenül utaló kifejezés használatára sor kerül.[24] Ez

[24] Belovics Ervin: Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények. In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál: Büntetőjog II. HVG-ORAC, Budapest, 2014. 286. o.

a hely a „más előtt", amely álláspontom szerint csak erősen áttételesen áll kapcsolatban a sértő tartalmat rögzítő adatok helyével, a lényege, hogy az elkövető cselekményének köszönhetően a jogsértő tartalom mások számára megismerhetővé váljon. Az elkövető erre alkalmas cselekményei többfélék lehetnek, így pl. a tények híresztelése a más által tett tényállítás továbbítása, amely lényegében eleve közvetítő tevékenységet jelöl.[25] Ezzel kapcsolatos a BH 2012.143. számú eseti döntés, amely szerint az újságban közölt cikknek honlapon, interneten történő ismételt megjelentetése híresztelésnek minősül, ugyanakkor az ügyben a jogsértő tartalom elhelyezésének helye – ugyan más okból – nem bírt jelentőséggel.

Az új jellegű illetékességi körülményt az eseti döntés azzal is indokolja, hogy a korábban elemzett, közléssel megvalósuló bűncselekményekkel szemben a rágalmazás és becsületsértés esetében a törvényi tényállásban célzat nem szerepel, a közlésnek nem is szükségszerű címzettje a sértett. Egyik bűncselekmény törvényi tényállásának maradéktalan megvalósulásához sem szükséges, hogy a becsület csorbítására alkalmas tényállítások vagy kifejezések a sértett tudomására jussanak, az csak a magánindítványhoz kötöttségük folytán a cselekmények büntethetőségének az előfeltétele. Az eseti döntés érvelése szerint a fentiekből az következik, hogy az interneten és egyúttal nagy nyilvánosság előtt elkövetett rágalmazás, illetve becsületsértés esetén a közzététel helye és egyben az elkövetés helye a weboldalt működtető szerver helye.

Az olyan felhő-alapú internetszolgáltatások esetén viszont, amikor egy adat helye nem határozható meg egyértelműen[26], ez a körülmény nem alkalmazható elsődleges illetékességi okként. Analógiával élve olyan helyzetet eredményezhet, mintha a nyomtatott sajtóban megjelenő közlés esetén az újság helyét határoznánk meg az elkövetés helyeként. Az eseti döntés az analóg formában elkövetett közlésekre kialakított joggyakorlathoz próbálta igazítani az új helyzetet, de attól is eltért. A döntés utalt az írott sajtóban, illetve rádiókban és televíziókban elkövetett becsületcsorbító cselekmények kapcsán egyöntetű azon gyakorlatra, miszerint az adott médium szerkesztőségének a székhelye határozza meg a büntetőügyben eljáró bíróság illetékességét, nincs ok ettől eltérni az elektronikus sajtó újabb formái, így az internet esetében sem. Ennek érvényre juttatása esetén a szervert üzemeltető vagy használó (hírközlési vagy információs társadalommal összefüggő szolgáltatást nyújtó) szolgáltató székhelye lenne irányadó.

[25] Belovics: i.m. 285. o.

[26] Nagy Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In: Homoki-Nagy Mária – Karsai Krisztina – Fantoly Zsanett – Juhász Zsuzsanna – Szomora Zsolt – Gál Andor (szerk.): Ünnepi kötet dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Szeged, 2018. 763-764. o.

Az eseti döntés – észlelve az internetes kommunikáció új helyzeteit – megfogalmazza az újszerű problémát, amely szerint számos, a magyar felhasználók által is széles körben látogatott honlap nem hazai szerverről működik. E helyzetet azonban a magánvádas eljárás illetékességi szabályaival oldja fel, nem az elkövetési magatartás értelmezésével.

5. Következtetések

Az elemzett bűncselekmények tekintetében az állapítható meg, hogy az internet valamennyi vizsgált esetben a bűncselekmény elkövetésének eszköze volt, a gyakorlatban mégis eltérő jelleget tulajdonítunk e technikai elemnek. Az illetékességet megalapozó körülmények eltérő rendezése bizonyára azzal van összefüggésben, hogy az elkövető tartózkodási helyének a vádemelés előtti meghatározása gyakorta nem megoldható, ezzel szemben a sértett tartózkodási helye a legtöbb esetben egyértelműen és kezdetektől fogva igen. A gyakorlat vizsgálata alapján úgy érezhető, hogy a jogalkalmazás máig nem tudja következetesen rendezni a hagyományos bűncselekmények internettel való kapcsolatát, azt bűncselekményenként eltérően próbálta az elkövetés értelmezésével vagy analógia útján a már kialakult dogmatikai rendszerhez igazítani.

Ez a törekvés azt hagyja figyelmen kívül, hogy az internet csupán eszköz. Rendkívül komplex, globális, megfoghatatlan, de ettől még eszköz. Az elkövetési magatartás következetes értelmezése esetén az internet nem lehet más, mint az elkövetés eszköze és nem pedig helye. Másként fogalmazva az elkövetés helyének meghatározása során az eszköz elkövető vagy a passzív alany általi igénybevételének helye lehet releváns, nem pedig az eszköz, illetve annak egy elemének – egyébként sem értelmezhető – helye.

A rágalmazás és becsületsértés esetében is igaz, hogy ezen eszköz igénybe vétele szükségszerűen csak az információs rendszer egyes rendszerelemein keresztül történhet, de éppen ezért ezen önállótlan elemekre nem építhető illetékességi ok. Az internetes bűncselekmények kapcsán felmerülő illetékességi kérdéseket ezért – az elkövetési magatartás helyes értelmezése mellett – a gyakorlati szempontokra és a technikai fejlődésre figyelemmel indokolt megválaszolni, erre láthatóan az eljárásjog alkalmas lehet.

Felhasznált Irodalom

Belovics Ervin: Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények. In: Belovics Ervin – Molnár Gábor Miklós – Sinku Pál: Büntetőjog II. HVG-ORAC, Budapest, 2014.

Dömölki Bálint (szerk.): Égen-földön informatika. Typotex, Budapest, 2008.

Eszteri Dániel: A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései. Infokommunikáció és jog. 2015/2-3.

Gibson, William: Neuromancer. Harper Collins, London. 1984.

Kincsei Attila: Technológia és társadalom az információ korában. In: Balogh G. (szerk.) Az információs társadalom, Gondolat-Új Mandátum, Budapest 2007.

Koppányi Szabolcs: Hírközlési jog az európai közösségben és Magyarországon, Osiris Kiadó Budapest, 2003.

Nagy Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In: Homoki-Nagy Mária – Karsai Krisztina – Fantoly Zsanett – Juhász Zsuzsanna – Szomora Zsolt – Gál Andor (szerk.): Ünnepi kötet dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Szeged, 2018.

Tóth András: Az elektronikus hírközlés és média gazdasági szabályozásának alapjai és versenyjogi vonatkozásai, HVG-ORAC Budapest, 2008.

Szerzők

Ambrus István kutató, Széchenyi István Egyetem, Deák Ferenc Állam- és Jogtudományi Kar, Bűnügyi Tudományok Tanszék; adjunktus, Eötvös Loránd Tudományegyetem, Állam- és Jogtudományi Kar, Büntetőjogi Tanszék; főtanácsadó, Kúria Büntető Kollégium

Csák Zsolt PhD. tanácselnök bíró, Kúria Büntető Kollégiuma; mb. óraadó, Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar, Büntető Anyagi, Eljárási és Végrehajtási Jogi Tanszék

Dornfeld László kutató, Mádl Ferenc Összehasonlító Jogi Intézet; doktorjelölt, Miskolci Egyetem Állam- és Jogtudományi Kar

Fenyvesi Csaba habil. egyetemi docens, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Büntető és Polgári Eljárásjogi Tanszék

Gyaraki Réka r. őrnagy, tanársegéd, Nemzeti Közszolgáti Egyetem Rendészettudományi Kar, Kiberbűnözés Elleni Tanszék

Herke Csongor DSc. tanszékvezető egyetemi tanár, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Büntető és Polgári Eljárásjogi Tanszék

Mezei Kitti tudományos segédmunkatárs, MTA Társadalomtudományi Kutatóközpont Jogtudományi Intézet; doktorjelölt, Pécsi Tudományegyetem Állam- és Jogtudományi Kar

Nagy Zoltán András tanszékvezető habil. egyetemi docens, Nemzeti Közszolgáti Egyetem Rendészettudományi Kar, Kiberbűnözés Elleni Tanszék; Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Büntetőjogi Tanszék

Simon Béla r. őrnagy, tanársegéd, Nemzeti Közszolgáti Egyetem Rendészettudományi Kar, Kiberbűnözés Elleni Tanszék

Szathmáry Zoltán PhD. ügyész, Legfőbb Ügyészség